
بسم الله
الرحمن الرحيم

Stake Hodler Capitalism: Blockchain and DeFi

(Decentralized Finance)

سرمایه‌داری سهام‌دار: بلاکچین و نظام مالی غیرمتمرکز

(امور مالی غیرمتمرکز)

نویسنده:

AMR WAHBA METWALI

تهیه و تدوین:

کارگزاری بانک انصار

مترجمان:

اشکان انتظام، ساناز ذبیحی، علی رضامنش، ریحانه روستایی، زهرا شیری، هما عزیزی، اکبر عباسی، رقیه عباسی، ویدا غلامی، مجید کریمی، تینوش مقدم راد و فرهاد مرسلی

عنوان: **Stake Hodler Capitalism: Blockchain and DeFi(Decentralized Finance)**
سرمایه‌داری سهام‌دار: بلاکچین و نظام مالی غیرمتمرکز(امور مالی غیرمتمرکز)
نویسنده: AMR WAHBA METWALI
تهیه و تدوین: **کارگزاری بانک انصار**
ویراستار: **پیام رنجبران**
طراح جلد و صفحه آرایی: **علیرضا خورسندی**
ناشر:
شمارگان: **۵۰۰ نسخه / چاپ اول ۱۴۰۰**
چاپ و صحافی:
بها: **ریال**
شابک: **۹۷۸-۹۶۴-۴۴۶**

فهرست مطالب

پیشگفتار

یکـی از دغدغه‌هـای کارگـزاری بانک انصار به عنوان یک نهاد پیشـرو در بازارسـرمایه، پاسـخگویی بـه مفاهیـم جدیـد در بازارهای مالـی اسـت. از مفاهیم جدیـد در بازارهای مالی جهـان، سـرمایه‌گذاری در بـازار رمزارزهـا اسـت. بنابراین شـناخت بسـتر این بازار و فلسـفه وجـودی آن بـرای هـر سـرمایه‌گذاری در ایـن حـوزه می‌توانـد حائـز اهمیـت باشـد. بـرای انجـام ایـن مهـم، معاونـت تحقیـق و توسـعه کارگـزاری بانـک انصار بـا همـکاری معاونت عملیـات بـازار بـه دنبـال یک منبع مناسـب و جامـع جهت آگاهی بخشـی به سـرمایه‌گذارن بودنـد، کـه در نهایـت کتاب «**سـرمایه‌داری سـهامدار: بلاکچیـن و نظام مالـی غیرمتمرکز (امـور مالـی غیرمتمرکـز[1])**» بـه عنوان یـک منبع مناسـب جهـت ترجمه انتخـاب گردید.

همانطـور کـه بیـان شـد، شـناخت بسـتر رمزارزهـا حائـز اهمیـت اسـت. بـلاک چیـن زیربنـای موفق‌تریـن پروژه‌هـای رمزارزهـا و یـک فنـاوری بـا آینـده کامـلا روشـن اسـت. ارزهـای دیجیتـال نویـن نظیر بیـت کویـن و اتریـوم، کـه روز بـه روز توجـه بسـیاری را بـه سـرمایه‌گذاری جلـب می‌کننـد، ویژگی‌هـای منحصربه‌فردشـان را مدیـون تکنولـوژی بلاکچیـن هسـتند. پروژه‌هـا و ایده‌هـای بسـیار خلاقانـه‌ای بر بسـتر آن شـکل گرفته و روز بـه روز کاربـرد بلاکچیـن در عرصه‌هـا و صنایـع مختلـف افزایـش پیـدا می‌کنـد. در فصـل اول ایـن کتاب سـعی شـده اسـت تمامـی آنچـه علاقه‌مندان در خصـوص این فنـاوری نیاز اسـت بداننـد را بطـور کامـل شـرح داده، بنابرایـن توصیـه مترجمـان ایـن اسـت حتما فصل اول را بدقـت مطالعـه نماییـد.

---

1. Stake hodler capitalism blockchain and defi (Decentralized finance)

در ادامـه بـه بررسـی فلسـفه وجودی بـازار رمزارزها پرداخته شـده اسـت. فلسـفه وجودی بـازار رمزارزهـا از بیـن بـردن سیسـتم مالـی متمرکـز اسـت. بازارهای مالـی که تا چند سـال قبـل بـا آن ها آشـنا بودیم، همگـی متمرکز بودنـد. در این بازارهـا، مقامات مرکـزی، ارز رایج را صـادر میکننـد کـه ایـن ارزها، باعـث حرکت رو به جلـوی اقتصاد میشـود و بـرای تمام داد و سـتد هـای بیـن دولت و بانکها اسـتفاده میشـوند. بنابراین، قـدرت مدیریـت و تنظیم جریان و عرضـه چنیـن ارزهایـی در بـازار، به دسـت نهاد مرکزی اسـت. ایـن امر مخاطراتـی را برای سـرمایه‌گذاران بوجـود مـی‌آورد، بنابرایـن به همین دلیل اسـت که سیسـتم مالـی غیرمتمرکز شـکل گرفـت. هـدف سیسـتم مالـی غیر متمرکـز [1]این اسـت کـه بـه سـرمایه‌گذاران کنترل کامـل دارایی‌هایشـان را بدهـد، و این می‌تواند بـه دلیل غیرمتمرکزسـازی و فناوری بلاکچین اسـتفاده شـده در آن باشد.

در همـه فصـل هـای این کتـاب دربـاره درک صحیح مفاهیـم اصلی فنـاوری بلاکچین، چگونگـی گسـترش آن در آینـده و تغییـر و تحولـی کـه در روند اجـرای فرایندهـای آنلاین بـه وجـود مـی‌آورد صحبـت کـرده اسـت. مفاهیـم ایـن کتـاب نشـان مـی دهـد کـه آینده اقتصـاد دنیـا چگونـه شـکل می‌گیـرد و بـه شـکل چشـمگیری همـه چیـز را ارتقـا خواهـد یافـت. نویسـنده ایـن کتـاب تلاش داشـته ضمن برشـمردن مزایایـی که فنـاوری بلاکچین بـه ارمغـان مـی‌آورد، چالش‌هـا و موانعـی کـه بر سـر راه توسـعه این فنـاوری وجـود دارد را نیـز بیـان کند.

ترجمـه ایـن کتاب تلاشـی اسـت، بـرای راهنمایـی افرادی کـه تنها در حد شـنیدن واژه رمـزارز یـا دنبال‌کـردن قیمـت ارزهـای دیجیتـال بـا ایـن فناوری آشـنا هسـتند و بـه دنبال شـناخت جنبه‌هـای بیشـتر و روش‌هـای سـرمایه‌گذاری در آنهـا می‌گردنـد.

اینجانـب و همکارانـم بـا هـدف ایفـای نقشـی کوچـک در مسـیر آرمـان پیشـرفت ایران سـربلند کوشـیدیم تـا بـا ترجمه کتابـی تحـت عنـوان، **سـرمایه‌داری سـهامدار: بلاکچین و نظـام مالـی غیرمتمرکز(امور مالی غیـر متمرکز)**، را تدوین و به اشـتراک بگذاریـم. امیدواریم کتـاب حاضـر بتوانـد سـهم کوچکی در آموزش داشـته و از سـوی مدیران در لایه‌ها و سـطوح مختلـف ملـی و سـازمانی، سیاسـت گـذاران و علاقه‌منـدان، داشـجویان علـم مدیریـت مالی مورد اسـتفاده قـرار بگیرد.

1. Defi

در ایـن بخـش لازم اسـت مراتـب سـپاس خـود را از همـکاران محتـرم خـودم کـه برای ترجمـه ایـن کتـاب زحمات بسـیار زیـادی کشـیدند، از آقایان علـی رضامنش، مجیـد کریمی، اکبرعباسـی، اشـکان انتظـام، تینـوش مقدمـراد و خانم‌هـا زهرا شـیری، سـانازذبیحی، ریحانه روسـتایی، همـا عزیـزی، رقیـه عباسـی و ویدا غلامـی به عمل رسـانم.

در پایـان امیـد دارم ایـن کتـاب کاربـردی بتوانـد در محیط‌هـای علمـی و انجمن‌هـای مالـی مـورد توجـه قرار گرفته و سـهم اندکی در مسـیر تبـادل اطلاعات و فراگیری اندیشـه‌ها داشـته باشد.

ارادتمند

امین آذریان

مقدمه

ورود به اکوسیستم بلاکچین، صرف‌نظر از پیشینهٔ هر شخص کمی دشوار و پیچیده به نظر می‌رسد. بیشتر افراد به همین دلیل امکان استفاده از فناوری بلاکچین و رمزارز را از دست می‌دهند، زیرا شناسایی فرصت‌های مبهم دشوار است. اصطلاحات به نظر فنی و گیج‌کننده هستند؛ بااین‌حال، بلاکچین یک فناوری جدید است که برای علاقه‌مندان به تمرکززدایی و کارایی، می‌تواند امیدوارکننده و جذاب باشد.

این کتاب مفاهیم فنی را در ساده‌ترین و خواندنی‌ترین قالب توضیح می‌دهد. شما مفاهیم اصلی فناوری بلاکچین را درک خواهید کرد. در پایان این کتاب، شما دانش کافی در مورد بلاکچین و نظام مالی غیرمتمرکز[1] را خواهید داشت که به شناسایی نقاط قوت، ضعف، فرصت‌ها و تهدیدها کمک می‌کند.

1. Decentralized Finance

یادداشت نویسنده

این مجموعه یکی از شاهکارهایی است که من به آن افتخار می‌کنم. من این موفقیت را نخست به خدا و سپس به مادر و همسرم، خانواده و دوستانم نسبت می‌دهم. بخش عمده‌ای از شخصیت امروز مرا، فوت پدرم در سال ۲۰۱۸ شکل داد. آنچه من را به‌عنوان فردی که اکنون هستم شکل داد، وقتی است که پدرم در سال ۲۰۱۸ درگذشت و این باعث شگفت‌زدگی من، دربارهٔ هدف واقعی زندگی شد؛ در آن زمان فهمیدم که لذت از سفر ناشی می‌شود و ارزشمندترین احساس از کمک به دیگران به دست می‌آید.

بلاکچین از تاریخ ۳۱ اکتبر ۲۰۰۸، وقتی ساتوشی ناکاموتو[1]، خالق بیت‌کوین، مقالهٔ خود را با عنوان سیستم نقدی الکترونیکی همتا همتا[2] منتشر کرد، در زندگی ما وارد شده است. با وجود این، بیت‌کوین تأثیر مستقیم خود را در زندگی من گذاشته است. من در سال ۲۰۱۷ درمورد بلاکچین و اکوسیستم مرتبط با آن تحقیق کردم. این زمانی بود که عاشق بلاکچین و نظام مالی غیرمتمرکز شدم. در این مجموعه، بیشتر به این موضوع خواهیم پرداخت که چرا من و بسیاری دیگر تا این حد به مبحث بلاکچین، رمزارزها و نظام مالی غیرمتمرکز علاقه‌مند شده‌ایم.

1. Satoshi Nakamoto
2. Peer-to-Peer

فصل ۱

برنامه‌های مالی غیرمتمرکز: برنامه‌های کاربردی جذاب خاص بلاکچین

چه در مورد نظام مالی غیرمتمرکز شنیده و چه در مورد آن نشنیده باشید، این امر کمابیش به‌طور مستقیم بخشی از زندگی روزمره ما شده است. در طول این فصل، ما اجزای نظام مالی غیرمتمرکز را به بخش‌های کوچکتر و قابل‌فهم تبدیل خواهیم کرد.

(DeFi) نظام مالی غیرمتمرکز چیست؟

نظام مالی غیرمتمرکز روشی است که توسط محققان مختلف، برای ایجاد یک نظام مالی جدید و باز طراحی شده است که هرکس می‌تواند بدون نیاز به واسطه‌های معتمد یا نهادهای واسط مانند بانک‌ها، کارگزاری‌ها یا صرافی‌ها به آن دسترسی پیدا کند. به نظر می‌رسد که رمزارزها بر پایهٔ بلاکچین یا فناوری دفتر کل توزیع‌شده[1] استوار هستند. امتیازهای ایجادشده توسط هریک از این اکوسیستم‌های کوچک که توسط رمزارزها تشکیل می‌شود، غیرقابل‌تصور است. هنوز هم بیت‌کوین اولین، شناخته‌شده‌ترین و بهترین نمونه است (گرچه بسیاری در حال حاضر آن را مانند طلا، ابزاری برای حفظ ارزش می‌دانند). پرداخت‌ها را می‌توان از طریق شبکه بیت‌کوین، به‌عنوان شبکه‌ای از گره‌های مستقل غیرمتمرکز برای تأیید معاملات انجام داد..

برای دستیابی به این هدف، نظام مالی غیرمتمرکز تا حد زیادی به رمزنگاری، بلاکچین و قراردادهای هوشمند[2] متکی است. قبل از معرفی این ایده به‌عنوان نظام مالی غیرمتمرکز، از آن

1. Distributed Ledger Technology
2. Smart Contracts

با عنوان نظام مالی باز[1] یاد می‌شد. یک قرارداد هوشمند، اصلی‌ترین سازهٔ نظام مالی غیرمتمرکز است. در نظام مالی غیرمتمرکز، بیشتر افراد مجاز به وام‌دهی یا وام‌گیری از دیگران، سفته‌بازی در دارایی‌های پایه مختلف با استفاده از قراردادهای مشتقات، معامله رمزارزها، پوشش ریسک و کسب سود از طریق سپرده‌ها هستند. در نظام مالی متمرکز، نسبت بالایی از سود به ریسک وجود دارد اما همراه با ریسک بالا است. بررسی بهترین پروژه‌های یک فرآیند دشوار است؛ اما درک اصول به شما کمک می‌کند تا بهترین تصمیم‌های سرمایه‌گذاری را در زمینهٔ بلاکچین و نظام مالی غیرمتمرکز بگیرید.

به نظر می‌رسد که رمزارزها مشابه نظام‌های بانکی سنتی عمل می‌کنند. وقتی صحبت از پرداخت می‌شود، می‌توانیم با بلاکچین به همان نتایج برسیم. نقطه قوت بلاکچین نسبت به سیستم‌های بانکی معمولی، ماهیت تغییرناپذیری و غیرمتمرکز آن است. تمرکززدایی می‌تواند صددرصد نسبت به آنچه امروزه سیستم‌های پرداخت سنتی ارائه می‌دهند، طیِ زمان به شما کمک کند. تغییرناپذیری بلاکچین عدم امکان تقلب را تضمین می‌کند. بیت‌کوین (گرچه اکنون بسیاری آن را مانند طلا وسیله‌ای برای حفظ ارزش می‌دانند) هنوز اولین و بهترین مثال است. «آلیس» می‌تواند بیت‌کوین به «بابفرد» دیگر پرداخت کند، بدون اینکه نیاز داشته باشد به یک واسطه مالی مانند بانک اعتماد کند.

در عوض، پرداخت‌ها می‌توانند از طریق شبکه بیت‌کوین انجام شوند؛ یعنی شبکه‌ای از درگاه‌های مستقل غیرمتمرکز برای تأیید معاملات. به‌طور خلاصه، برای وقوع همهٔ این موارد، نظام مالی غیرمتمرکز به‌شدت به رمزارزها، بلاکچین و قراردادهای هوشمند متکی است. اگر نمی‌دانید قرارداد هوشمند چیست یا چگونه به‌سادگی کار می‌کند، نگران نباشید. ما قراردادهای هوشمند را در فصل ۳ این کتاب مرور خواهیم کرد.

رمزنگاری[2]

رمزگذاری[3] به‌عنوان مؤلفه اصلی رمزنگاری در نظر گرفته می‌شود. به‌طورکلی، رمزگذاری ایجاد و تجزیه و تحلیل پروتکلی است که از خواندن یا دسترسی اشخاص ثالث یا مردم به اطلاعات ذخیره‌شده یا انتقال یافته، از طریق یک رسانه ارتباطی جلوگیری می‌کند. قالب قابل خواندن

1. Open Finance
2. Cryptography
3. Encryption

برای رمزگذاری، تعریف یک جعبه سیاه است که شما یک داده را وارد می‌کنید و از یک کلید برای رمزگذاری آن استفاده می کنید؛ و این فرایند را نمی‌توان تغییر داد، مگر با یک کلید منحصربه‌فرد که دو یا چند طرف می‌توانند به اشتراک بگذارند.

در قلب رمزگذاری مدرن، جنبه‌های مختلف امنیت اطلاعات مانند محرمانه بودن داده‌ها، صداقت، اصالت و عدم انکار وجود دارد. رمزنگاری مدرن در تقاطع ریاضیات، علوم کامپیوتر، مهندسی برق، ارتباطات و فیزیک است. برنامه‌های رمزنگاری شامل تجارت الکترونیکی، کارت‌های بدهی مبتنی بر تراشه، ارزهای دیجیتال، رمزنگاری رایانه‌ای و ارتباطات نظامی می‌شود.

قبل از دوران مدرن، رمزنگاری عبارت بود از تبدیل اطلاعات قابل خواندن به عبارت‌های غیرقابل خواندن. فرستنده‌های پیام رمزگذاری‌شده، از رمزگشاها فقط برای گیرندگان مورد نظر خود استفاده می‌کنند و این امر باعث می‌شود تا حملات غیرممکن شوند. در ادبیات رمزنگاری، اغلب نام‌های آلیس (A) برای فرستنده، باب (B) برای گیرندهٔ مورد نظر و ایو (Eve(Block برای مهاجم (هکر) استفاده می‌شود. از زمان توسعه ماشین‌های رمزگذاری در طول جنگ جهانی اول و ظهور رایانه‌ها در طول جنگ جهانی دوم، فناوری رمزگذاری پیچیده‌تر و نرم‌افزارهای آن متنوع‌تر شده است.

رمزنگاری مدرن اساساً بر پایهٔ نظریه‌های علوم ریاضی و رایانه است. الگوریتم‌های رمزنگاری بر اساس مفروضات مربوط به امنیت رایانه طراحی شده‌اند و بهره‌برداری از این الگوریتم‌ها کار را برای مهاجمان (هکرها) دشوار می‌کند. هک کردن سیستمی که خوب طراحی شده باشد تقریباً غیرممکن است؛ اما در عمل با رایانه‌های کوانتومی امکان‌پذیر است، ولی این موضوعی است که از حوصلهٔ این کتاب خارج است. در حال حاضر، بیایید به استفاده از رمزنگاری به‌عنوان مطمئن‌ترین راه برای ذخیره و انتقالِ داده فکر کنیم؛ ازاین‌رو، این سیستم‌ها اگر به‌خوبی طراحی شده باشند «امنیت داده» نامیده می‌شوند.

با توجه به پیشرفت‌های نظری مانند پیشرفت در الگوریتم‌های تجزیهٔ عدد صحیح و تکنیک‌های محاسباتی سریع‌تر، این طرح‌ها باید دائماً بررسی و در صورت لزوم اصلاح شوند. اگرچه از نظر تئوری، قطع مدارهای امن حتی با توان محاسباتی نامحدود، مانند دکمه‌های یک‌بارمصرف، غیرممکن است؛ اما این مدارها از نظر تئوری بهترین هستند ولی استفاده از آن‌ها در عمل بسیار دشوارتر از رایانه‌های مدار ایمن است.

پیشرفت فناوری رمزگذاری بسیاری از مسائل حقوقی درباره حریم خصوصی را در عصر اطلاعات به وجود آورده است. به دلیل امکان استفاده از رمزنگاری در جاسوسی، فعالیت‌های

غیرقانونی و سایر برنامه‌های تقلبی، بسیاری از دولت‌ها آن را به‌عنوان یک سلاح طبقه‌بندی کرده‌اند و استفاده و صادرات آن را محدود یا حتی ممنوع کرده‌اند. برای مثال «اسکایپ» از پیاده‌سازی اختصاصی الگوریتم رمزگذاری[1] استفاده می‌کند. اگر نمی‌دانید این استاندارد به چه معناست، نکته مهمی که باید درک کنید این است که رمزنگاری، همان چیزی است که حریم خصوصی و ایمنی ما را در این عصر اطلاعات تضمین می‌کند.

برخی حوزه‌ها که استفاده از رمزگذاری در آن‌ها قانونی است، ممکن است قانونگذاران را ملزم به افشای کلیدهای رمزگذاری برای برخی از اسناد کنند. رمزگذاری همچنین در مدیریت حقوق دیجیتال و اختلافات درمورد نقض حق چاپ، در رسانه‌های دیجیتال نقش مهمی دارد. مدت‌هاست که آژانس‌های اطلاعاتی و مراکز اجرای قانون، علاقه‌مند به رمزگذاری هستند. ارتباطات محرمانه می‌تواند جنایی یا کلاهبرداری باشد؛ در نتیجه تاریخچه‌ای از مسائل حقوقی متناقض با رمزگذاری وجود دارد، به‌ویژه با ظهور رایانه‌های کم هزینه که رمزگذاری با کیفیت بالا را به‌طور گسترده‌تر در دسترس قرار می‌دهد.

در بعضی از کشورها حتی استفاده داخلی از رمزگذاری محدود شده است. تا سال ۱۹۹۹، فرانسه رمزنگاری را به‌شدت در مرزهای خود محدود می‌کرد؛ اما بعدها بسیاری از قوانین را لغو کرد. در چین و ایران، هنوز برای رمزگذاری مجوز لازم است. بسیاری از کشورها محدودیت‌های شدیدی در استفاده از رمزگذاری به‌ویژه در ایجاد کانال‌های ارتباطی دارند.

اگرچه رمزگذاری برای مصارف غیرکاری در ایالات متحده قانونی است؛ اما همواره اختلافات زیادی بر سر مسائل حقوقی مربوط به رمزگذاری وجود داشته است. یکی از مهمترین موارد، صادرات نرم‌افزارها و ابزارهای رمزگذاری بود. شاید علت آن، نقش و اهمیت رمزنگاری در طول جنگ جهانی دوم باشد و تصور اینکه رمزنگاری برای امنیت ملی اهمیت دارد.

پس از جنگ جهانی دوم، فروش یا توزیع فناوری رمزنگاری در خارج از کشور در ایالات متحده غیرقانونی بود. رمزگذاری به‌عنوان تجهیزات نظامی تعیین و در فهرست ارتش ایالات متحده قرار گرفت. پیش از ظهور رایانه‌های شخصی، الگوریتم‌های کلید نامتقارن (برای مثال، روش‌های کلید عمومی) و اینترنت، این مسئله چندان با اهمیت نبود؛ بااین‌حال، با رشد اینترنت و دسترسی بیشتر به ابزارهای محاسباتی و قدرت اینترنت، روش‌های رمزگذاری با کیفیت بالا در سراسر جهان شناسایی و معرفی شدند.

1. Advanced Encryption Standard (AES)

فصل ۲

بلاکچین

بلاکچین نوع خاصی از پایگاه داده است که داده‌ها و اطلاعات را به‌صورت متفاوت ذخیره می‌کند. در فضای بلاکچین، داده‌ها به شکل بلوک‌های به‌هم‌پیوسته ذخیره می‌شوند. بلوک‌ها شامل مجموعه‌هایی از اطلاعات هستند که در گروه‌هایی جداگانه (به آن‌ها بلوک می‌گویند) ذخیره می‌شوند. هر بلوک ظرفیت مشخصی از حافظه دارد و هنگامی که این ظرفیت پُر می‌شود، به بلوک‌های پُر شدهٔ قبلی پیوند داده می‌شود، تا به‌صورت یک زنجیره از اطلاعات درآیند که به آن‌ها بلاکچین گفته می‌شود. تمام اطلاعات جدید پس از تشکیل یک بلوک به زنجیره اطلاعات بلوکی ماقبل خود می‌پیوندد و این فرآیند تا بی‌نهایت و به‌طور نامحدود ادامه می‌یابد.

بلاکچین به نظر پیچیده می‌رسد؛ اما اگر بخواهیم به زبان ساده و قابل‌فهم تعریفش کنیم: بلاکچین یک زنجیره از لینک‌های کوچک به‌هم‌پیوسته است. هر لینک شامل اطلاعاتی مانند تراکنش‌های بانکی یا اسناد مالکیت، قراردادها، پیام‌های شخصی، ویدیو، موزیک یا دیگر اطلاعات است. برای فهم دقیق بلاکچین ابتدا باید بدانید پایگاه داده چیست.

پایگاه داده در واقع یک مجموعه از اطلاعات الکترونیکی یا دیجیتال است، که در یک سیستم کامپیوتری ذخیره شده است. اطلاعات یا داده‌ها در جداول یک پایگاه داده ذخیره می‌شوند تا به آسانی قابل جست‌وجو و بازیابی باشند.

تفاوت بین یک صفحه گسترده[1] مانند فایل‌های اکسل و یک پایگاه داده در همین جاست. یک صفحه گسترده برای کاربران یا گروه‌های کوچکتری طراحی شده است که به ذخیره و دسترسی مقدار محدود و معینی از اطلاعات دسترسی و نیاز دارند؛ درحالی‌که پایگاه داده‌ها برای

1. Spreadsheet

ذخیره، جست‌وجو و بازیابی حجم بیشتری از اطلاعات قابل اصلاح، توسط چند کاربر، به‌صورت همزمان طراحی شده است.

پایگاه داده‌های بزرگ برای این کار به سرورهای قدرتمندی دسترسی دارند، که در برخی موارد این سرورها از صدها و گاه هزاران کامپیوتر تشکیل شده‌اند که توان و حافظه مورد نیاز این فرآیند را برای دسترسی چندین کاربر به‌طور همزمان، در حداکثرِ کارایی زمانی ممکن فراهم می‌کنند. وقتی که افراد زیادی به یک صفحه گسترده یا پایگاه داده دسترسی دارند، معمولاً تحت مدیریت افراد تعیین‌شده‌ایی هستند که بر کار آنها تسلط کامل دارند.

زمانی که داده جدیدی وارد بلاکچین می‌گردد، وارد بلوک‌های جدید می‌شود و زمانی که یک بلوک پُر می‌شود به بلوک‌های ماقبل خود زنجیر می‌شود. این اتصال به ترتیب زمان وقوع شکل می‌گیرد. انواع مختلفی از داده می‌تواند در یک بلاکچین ذخیره شود؛ اما معمول‌ترین، رایج‌ترین و پرکاربردترین نوعِ داده، اسناد تراکنش‌های مالی (دفترکل تراکنش‌ها) در بیت‌کوین یا سایر رمزارزها است.

هنگامی که در مورد بیت‌کوین صحبت می‌کنیم، بلاکچین به‌صورت غیرمتمرکز استفاده می‌شود؛ به‌نحوی که تحت کنترل هیچ شخص یا گروه خاصی نیست و درعین‌حال، همهٔ کاربران آن را کنترل می‌کنند. این بلاکچین غیرمتمرکز، قابل دست‌کاری نیست؛ بنابراین همهٔ اسناد ذخیره شده، غیرقابل بازگشت هستند. در مورد بیت‌کوین، به این معنی است که همهٔ افراد به‌صورت پیوسته در حال ثبت تراکنش‌های خود در سیستم هستند.

جنبه مهمی که بیشتر افراد قادر به درک آن نیستند این موضوع است که چگونه این بلاک‌ها به این زنجیره اضافه می‌شوند. پاسخ این سؤال را باید در مفهومی به نام «استخراج» جست‌وجو کرد. در ساده‌ترین تعریف، استخراج تأیید مشروعیت و قانونی بودن و سلامت یک بلوک قبل از اتصال به بلاکچین است. این فرآیند به‌وسیلهٔ مشارکت دادن گره‌ها انجام می‌پذیرد که به‌صورت اتفاقی انتخاب می‌شوند و در برگشت، یک بلوک به‌عنوان پاداش دریافت می‌کنند. در بخش ۶ به‌طور کامل به مبحث استخراج می‌پردازیم.

بعد از تعریف این مفاهیم این سؤال به ذهن می‌رسد که وجه تمایز بلاکچین و پایگاه داده چیست؟ در ادامه به تشریح این تفاوت‌ها می‌پردازیم.

ساختار مستحکم

تفاوت اساسی بین پایگاه داده معمولی و بلاکچین در چگونگی ساختاربندی داده‌هاست.

بلاکچین داده را در یک بلوک گردآوری می‌کند که شامل مجموعه‌ای از اطلاعات هستند. بلوک‌ها ظرفیت مشخصی دارند و زمانی که پُر می‌شوند به زنجیرهٔ بلوک‌های پُر شدهٔ قبل از خود می‌پیوندند و به همین صورت پیش می‌روند تا یک زنجیره از بلوک‌ها شکل بگیرد که به آن بلاکچین می‌گوییم. همهٔ این اطلاعات جدید که بعد از این بلوکِ تازه اضافه‌شده می‌آیند، در این بلوک تازه ذخیره می‌شود که این بلوک هم پس از پُر شدن به زنجیرهٔ بلاکچین الحاق می‌گردد.

ولی در پایگاه داده، داده‌ها در جداول ساختاربندی می‌شوند. در بلاکچین همان گونه که از نامش برمی‌آید داده‌ها در قالب بلوک‌هایی ذخیره می‌شوند که به‌هم می‌پیوندند؛ ازاین‌رو همهٔ بلاکچین‌ها می‌توانند به‌عنوان یک پایگاه داده در نظر گرفته شوند؛ اما همهٔ پایگاه داده‌ها نمی‌توانند یک بلاکچین باشند. این سیستم همچنین یک خط زمانی غیرقابل‌بازگشت از داده‌هاست که در یک فضای غیرمتمرکز اجرا شده است.

لحظه‌ای که یک بلوک پُر می‌شود به‌صورت خودکار بخشی از این خط زمانی می‌گردد. هر بلوک در زنجیره اطلاعات، برچسب زمانی خود را می‌گیرد و در آنجا می‌نشیند.

تمرکززدایی

همانند یک پایگاه داده، بیت‌کوین نیز برای ذخیره بلاکچین به مجموعه‌ای از رایانه‌ها نیاز دارد. در خصوص بیت‌کوین، بلاکچین نوعی پایگاه داده بوده که تمامی معاملات بیت‌کوین ملحق شده به مجموعه بلوک‌ها را، در خود جای داده است. در مورد بیت‌کوین و برخلاف اکثر پایگاه‌های داده، همهٔ رایانه‌ها در یک محل واحد و زیر یک سقف مستقر نیستند و هر رایانه یا گروهی از رایانه‌ها، توسط فرد یا گروهی متفاوت از افراد دیگر اداره می‌شود.

فرض کنید یک شرکت دارای یک سرور با حدود ده‌هزار کامپیوتر با یک پایگاه داده است، که اطلاعات حساب تمام مشتریان شرکت را در خود جای داده است. این شرکت صاحب انباری است که همهٔ این رایانه‌ها را زیر یک سقف جمع کرده و کنترل و دسترسی کامل به هریک از این رایانه‌ها و کلیهٔ اطلاعات آن‌ها را در اختیار دارد. به همین ترتیب، بیت‌کوین از هزاران رایانه تشکیل شده است که هر رایانه یا مجموعه‌ای از رایانه‌ها، بلاکچین آن را در خود جای داده‌اند. این رایانه‌ها در مکان‌های جغرافیایی مختلفی قرار دارند و هر یک یا گروهی از آن‌ها، توسط افراد یا گروه‌های مختلفی اداره می‌شوند. این رایانه‌ها به‌عنوان شبکه بیت‌کوین، تحت‌عنوان گره شناخته می‌شوند.

بنابراین، بلاکچین بیت‌کوین به‌صورت غیرمتمرکز استفاده می‌شود؛ بااین‌حال، بلاکچین‌های

خصوصی و متمرکز که رایانه‌ها شبکهٔ آن‌ها را تشکیل می‌دهند، توسط یک عامل واحد کنترل می‌شوند. بلاکچین‌های خصوصی می‌توانند متناسب با نیازهای تجاری شما به کار گرفته شوند و درعین‌حال دسترسی اطلاعات برای عموم را به حداقل می‌رسانند. نمونه‌هایی از سیستم عامل‌هایی که راه‌حل‌های بلاکچین خصوصی ارائه می‌دهند، عبارت‌اند از:

«Blockchain IBM Blockchain»،

«Azure Blockchain» و

(AWS)” Amazon Web Services».

در بلاکچین، هر گره، تاریخچهٔ کاملی از داده‌های بلاکچین از بدو تولد را دربردارد. در خصوص بیت‌کوین، داده‌ها، تاریخچهٔ کاملی از تمام معاملات بیت‌کوین است؛ بنابراین اگر در داده‌های یک گره خطایی وجود داشته باشد، می‌تواند از هزاران گره دیگر به‌عنوان مرجع برای اصلاح خود استفاده کند. به این ترتیب، یک گره در شبکه، هیچ‌یک از اطلاعات درون آن را تغییر نمی‌دهد؛ در نتیجه تاریخچهٔ معاملات در هر بلوک بلاکچین بیت‌کوین تغییرناپذیر است.

اگر کاربری قصد تغییر سابقهٔ معاملات بیت‌کوین را داشته باشد، گره‌های دیگر به‌راحتی با مراجعه به مرجع داده، گره دست‌کاری‌شده را تشخیص می‌دهند. این سیستم به ساخت ترکیبی دقیق و شفاف از رویدادها کمک می‌کند. در خصوص بیت‌کوین اطلاعات مانند فهرست معاملات است؛ بااین‌حال، احتمالاً وظیفهٔ یک بلاکچین است که قراردادهای مختلف حقوقی، اطلاعات هویتی محلی یا موجودی محصولات یک شرکت را ذخیره کند. قابلیت ثبت تغییرات چند شبکهٔ غیرمتمرکز باید گردآوری شده تا خروجی دیگری از عملکرد سیستم، یا اطلاعات موجود در آن دریافت گردد. با این کار اطمینان حاصل می‌شود تمامی تغییرات، به سود اکثریت است.

شفافیت

به دلیل ماهیت غیرمتمرکز بودن بلاکچین بیت‌کوین، هریک از مبادلات، فارغ از گره مختص خود یا استفاده از جست‌وجوگر بلاکچین، به‌وضوح و زنده دیده می‌شوند. هر گره، دارای نسخهٔ خاصی از زنجیره است که پس از تأیید بلوک‌های جدید به‌روز می‌شود؛ بنابراین، در صورت نیاز، قادر به ردیابی بیت‌کوین در هر مسیری هستید؛ برای مثال، مبادلات رمزارزهای هک‌شده‌ای که دارنده بیت‌کوین همه چیز را از دست داده است. اگرچه ممکن است هکر ناشناخته باشد اما بیت‌کوین‌های به سرقت رفته کاملاً قابل ردیابی هستند. در صورت انتقال یا ذخیرهٔ بیت‌کوین‌های دزدیده شده، مالک اصلی می‌تواند آن‌ها را ردیابی کند. مفهومی نیز هست

به نام رنگ کردن سکه[1]، و این همان رنگ کردن پولی است که از بانک ها دزدیده می‌شود.

امنیت بلاکچین چقدر است؟

فناوری بلاکچین موضوع امنیت و اعتماد را از راه‌های مختلف در نظر می‌گیرد. نخست، بلوک‌های جدید همیشه در یک مسیر مستقیم و منظم قرار می‌گیرند. آن‌ها همیشه به انتهای بلاکچین اضافه می‌شوند. اگر به‌دقت به بلاکچین بیت‌کوین نگاه بیندازید، متوجه می‌شوید که هر بلوک جای مشخصی روی زنجیره دارد که به آن «ارتفاع[2]» می‌گویند. ارتفاع بلاکچین در حال حاضر به حدود ۱۹۷،۶۵۶ بلوک رسیده است.

پس از قراردهی یک بلوک در انتهای بلاکچین، جابه‌جایی و تغییر در محتوای بلوک بسیار دشوار است، مگر اینکه اکثر کاربران برای انجام این کار توافق کنند. به این دلیل است که هر بلوک از کد هش[3] آن تشکیل شده است؛ مانند ۰۰۰۰۰۰۱۳۹۳ nd5n3v32d134d214n14m02018 به‌علاوه هش بلوک قبل از آن.

کد هش چیست؟ کدهای هش با یک تابع ریاضی ساخته می‌شوند که اطلاعات دیجیتالی را به دنباله‌ای از اعداد و حروف تبدیل می‌کنند که وقتی از طریق ابزارهای خاص وارد آن شوید، می‌توانید آن‌ها را تفسیر کنید. اگر اطلاعات به هر طریقی تغییر کند، کد هش نیز تغییر خواهد کرد. این مسئله در راستای ارتقای امنیت صورت می‌گیرد.

فرض کنید یک هکر می‌خواهد بلاکچین را تغییر دهد و بیت‌کوین را به‌طور غیرقانونی از باقی افراد حاضر در پلتفرم سرقت کند. اگر هکر روی نسخهٔ اصلی تغییری ایجاد کند، آن نسخه دیگر با نسخهٔ دیگران ارتباط برقرار نمی‌کند؛ بنابراین هنگامی که کاربران دور هم جمع شده تا نسخه‌های خود را با دیگران مقایسه کنند، متوجه تفاوت نسخه می‌شوند؛ در نتیجه بلوک هکر به‌عنوان غیرمجاز طبقه‌بندی و شناسایی می‌گردد.

هکر برای موفقیت در این عملیات، باید حداقل ۵۱ درصد از نسخه‌های بلاکچین را یکی پس از دیگری کنترل و تغییر دهد تا نسخهٔ جامع جدید به نسخهٔ اصلی تبدیل شود. برای موفقیت در چنین حمله‌ای، به‌مقدار زیادی پول و منابع برای ساخت مجدد تمام بلوک‌ها از ابتدا تا انتها نیاز دارد؛ زیرا کدهای هش و سیرهای زمانی[4] متفاوتی پس از تغییر ایجاد می‌گردد.

---

1. Tainting coins
2. Height
3. Hash
4. Timestamps

اندازه و رشد سریع شبکهٔ بیت‌کوین و هزینهٔ انجام چنین معامله‌ای بسیار زیاد و غیرممکن و به اندازهٔ بمب اتم مخرب است. پیشبرد چنین عملیاتی را نمی‌توان از سایر کاربران پنهان کرد؛ زیرا هرگونه تغییر فاحش در بلاکچین قابل مشاهده است. اعضای شبکه بلافاصله به قسمت جدیدی از بلاک‌چین جابه‌جا می‌شوند که تخریب و دست‌کاری نشده است.

این امر باعث کاهش ارزش قسمت مورد حمله می‌گردد، و در نهایت حمله بی‌اثر می‌شود چون بازیگر (هکر)، کنترل چیزی جز یک سرمایه‌گذاری بی‌ارزش را به دست نیاورده است. چنانچه هکر قصد حمله به نسخه جدید بیت‌کوین را داشته باشد، همین اتفاق دوباره تکرار می‌شود. این پلتفرم به‌گونه‌ای طراحی شده است که ماندن به‌عنوان بخشی از شبکه بسیار اقتصادی‌تر از حمله به آن است.

مقایسه بیت‌کوین با بلاکچین

هدف بلاکچین ثبت و به اشتراک‌گذاری اطلاعات دیجیتال بدون تغییر آن‌هاست. فناوری بلاکچین اولین بار در سال ۱۹۹۱ توسط «استوارت هابر» و «دبلیو اسکات استورنتا» مطرح شد. این دو محقق می‌خواستند سیستمی راه‌اندازی کنند که غیرقابل دست‌کاری باشد؛ بااین‌حال، تنها دو دهه بعد بود که بلاکچین اولین بار با «بیت‌کوین» به یک تجربهٔ واقعی تبدیل شد.

کاربری بیت‌کوین بر روی بلاکچین طراحی شده است. در یک مقالهٔ تحقیقاتی درباره معرفی ارز دیجیتال، بنیانگذار بیت‌کوین، «ساتوشی ناکاموتو[1]»، از آن به عنوان یک سیستم پول الکترونیک جدید کاملاً «کاربر به کاربر» بدون هرگونه واسطه‌ای نام برد.

نکته اساسی اینجاست که تنها هدف بلاکچین، ثبت حساب‌های یک دفتر کل برای بیت‌کوین نیست؛ اما بلاکچین می‌تواند برای ثبت کاملِ بی‌نهایت داده مورد استفاده قرار گیرد؛ برای مثال، می‌تواند این‌طور باشد که برای ثبت معاملات پولی رایج، آرای انتخابات، موجودی کالا، شناسه‌های دولتی، اسناد خانه و غیره به کار گرفته شود.

در حال حاضر، طیف گسترده‌ای از پروژه‌های مبتنی بر بلاکچین هست که از بلاکچین نه فقط برای ثبت معاملات، بلکه برای کمک به جامعه استفاده می‌کنند. برای مثال، بلاکچین همچون ابزاری برای رأی دادن در انتخابات دموکراتیک مورد استفاده قرار می‌گیرد. ماهیت تغییرناپذیر و ثبات بلاکچین باعث می‌شود که رأی‌گیری غیرقانونی کمی سخت‌تر باشد.

1. Satoshi Nakamato

یک سیستم رأی‌گیری می‌تواند به‌گونه‌ای عمل کند که هر شهروند یک کشور، یک رمزارز یا توکن اختصاصی داشته باشند؛ سپس به هر کاندیدا یک آدرس کیف پول خاص اختصاص می‌یابد، و رأی‌دهندگان رمزارز یا توکن اختصاصی خود را به آدرس کیف پول کاندیدای مورد نظر خود ارسال می‌کنند. قابلیت پیگیری و شفافیت بلاکچین نیاز به حضور انسان برای شمارش آرا را برطرف می‌کند و از مداخله هکرها در شمارش آرای فیزیکی جلوگیری می‌کند.

روش‌های اجرای بلاکچین

بلوک‌های بلاکچین بیت‌کوین، حاوی داده‌هایی درباره مبادلات پولی هستند. بااین‌حال، مشخص است که بلاکچین روشی قابل اعتماد برای نگهداری اطلاعات در مورد انواع دیگر معاملات نیز هست.

برخی شرکت‌ها که در حال حاضر بلاکچین را اجرا می‌کنند، عبارت‌اند از: "Walmart"، "Pfizer"، "AIG"، «Siemens»، "Unilever" و بسیاری از شرکت‌های دیگر. به‌عنوان مثال، "IBM" برای دنبال کردن مسیر محصولات غذایی خود در محدوده جغرافیایی خاصی، سیستم "Food Trust Blockchain" را طراحی کرده است.

چرا این لازم است؟ صنایع غذایی شاهد شیوع‌های بی‌شماری از «E. coli»، سالمونلا، لیستریا، و مواد سمی بوده است که به اشتباه به غذاها نسبت داده شد. پیش از این، کشف هستهٔ اصلی آن یا منشأ بیماری‌هایی که از غذا به انسان منتقل می‌شد، هفته‌ها طول می‌کشید.

با استفاده از بلاکچین، برندها امکان ردیابی محصولات غذایی خود از مبدأ، مسیر و مقصد نهایی را دارند. اگر غذایی آلوده باشد، می‌توان آن را به مبدأ بازگرداند. به‌علاوه، این شرکت‌ها می‌توانند با شناسایی یا پیش‌بینی یک مشکل و برقراری تماس، یک زندگی را نجات دهند. ما در قسمت ۳ «Stake Hodler Capitalism: Blockchain and IoT»، بیشتر به نمونه‌ها و کاربرد بلاکچین خواهیم پرداخت.

این نمونه‌ای کاربردی از بلاکچین بود؛ اما موارد دیگری از انواع اجرای بلاکچین وجود دارد. در اینجا به کاربردهای بیشتری از بلاکچین خواهیم پرداخت.

بانکداری و امور مالی

شاید هیچ صنعتی به‌اندازهٔ بانکداری امکان استفاده از بلاکچین را در عملیات تجاری خود نداشته باشد. مؤسسات مالی فقط می‌توانند در ساعت‌های کاری و پنج روز در هفته کار کنند.

این بدان معنی است که اگر بخواهید مبلغی را در ساعت شش عصر روز جمعه پرداخت کنید، شما باید تا صبح روز دوشنبه صبر کنید تا وجه به حساب واریز شود. حتی اگر انتقال وجه شما در ساعت و روز کاری صورت گیرد، ممکن است به‌علت حجم بالای تراکنش‌های بانکی، لازم باشد یک تا سه روز کاری صبر کنید تا تراکنش تأیید شود. از طرف دیگر، بلاکچین هرگز نمی‌خوابد و استراحت نمی‌کند. در داخل اکوسیستم بلاکچین، هر دقیقه از تمام روزهای هفته، ساعت کاری محسوب می‌شود.

با ورود بلاکچین به سیستم بانک‌ها، اکنون کاربران می‌توانند در کمتر از ده دقیقه، شاهد پردازش تراکنش‌های خود باشند. همچنین بانک‌ها با استفاده از بلاکچین این امکان را دارند که مبادلات بین مؤسسات را با سرعت و امنیت بیشتری انجام دهند؛ برای مثال، در فرایند معاملات سهام، روند تسویه می‌تواند تا سه روز یا در صورتی که معامله بین‌المللی باشد بیش از سه روز طول بکشد. این بدان معنی است که پول و سهام در این مدت غیرقابل دسترسی هستند. حال با کمک قراردادهای هوشمند، این سیستم‌های مالی را می‌توان توسط مجموعه‌ای از قوانین و مقررات از پیش تعریف و کدگذاری‌شده، به‌نحو کاملاً مستقل اداره کرد. اطلاعات بیشتر در خصوص این نوع قراردادهای هوشمند در فصل ۳ ارائه می‌شود.

در مورد تراکنش‌ها، حتی چند روزی که پول در حال انتقال است، بانک با هزینه‌های اساسی و ریسک‌هایی روبه‌رو است. ازاین‌رو، بانک اروپایی «سانتاندر» و شرکای تحقیقاتی آن، صرفه‌جویی احتمالی حدود پانزده تا بیست میلیارد دلار در سال را اعلام کردند. طبق محاسبات «کاپگمینی»، یک مشاور فرانسوی، به کمک برنامه‌های مبتنی بر بلاکچین، هر ساله تا شانزده میلیارد دلار در هزینه‌های بانکی و بیمه‌ای صرفه‌جویی می‌شود.

واحد پول

بلاکچین اساس ارزهای رمزنگاری‌شده مانند بیت‌کوین را شکل می‌دهد. «فدرال رزرو» دلار آمریکا را کنترل می‌کند. در این سیستم قدرتمند مرکزی، پول و اطلاعات کاربران تحت امنیت بانک یا دولت است. اگر بانک کاربر هک شود در این صورت اطلاعات شخصی مشتری در خطر است. اگر عملکرد بانک مشتری مختل شود یا در کشوری با دولت بی‌ثبات زندگی کند، ممکن است ارزش پول او در معرض خطر باشد. در سال ۲۰۰۸، برخی از بانک‌هایی که پول کم آورده بودند با استفاده از مالیات‌های پرداختی مردم نجات پیدا کردند. این‌ها دغدغه‌ها و نگرانی‌هایی بود که منجر به تولد بیت‌کوین شد.

بلاکچین با توزیع عملکرد خود در شبکهٔ گره‌ها، به بیت‌کوین و سایر رمزارزها توانایی فعالیت بدون نیاز به یک قدرت مرکزی را می‌دهد. این نه‌تنها ریسک را به حداقل می‌رساند، بلکه مقدار زیادی از هزینه‌های پردازش تراکنش‌ها را نیز حذف می‌کند. کسانی که در کشورهایی با سیستم ارزی یا زیرساخت‌های مالی بی‌ثبات و نامنظم زندگی می‌کنند، می‌توانند با پیوستن به برنامه‌های بیشتر و شبکه‌های گسترده‌ای از کاربران و مؤسسات، با انجام تراکنش‌ها و مبادلاتی در داخل یا خارج از کشور، به ثبات ارزی دست یابند. با این اوصاف، رمزارزها با مخالفت‌های زیادی روبرو شده‌اند و برخی ادعا می‌کنند که این می‌تواند جایگزینی برای دلار باشد. هنوز هم، اگر با دقت بیشتری به قضیه فکر کنیم، درمی‌یابیم که ایدهٔ دلار رمزنگاری‌شدهٔ ایالات متحده، به‌عنوان یک اکوسیستم کوچک از رمزارزها بسیار قابل دستیابی است. بیایید ترس از محاسبات کوانتومی را کنار بگذاریم که مانع رمزنگاری است. چنین حملاتی انجام‌ناپذیر است. علاوه بر موارد ذکر شده در بالا، اهمیت تصمیم‌گیری یک دولت درباره استفاده از رمزارزها، به همان اندازهٔ تصمیم‌گیری در خصوص استفاده از سلاح هسته‌ای است.

با ارز رمزنگاری‌شده، کیف پول برای حساب‌های پس‌انداز یا به‌عنوان وسیلهٔ پرداخت بسیار مورد استقبال است، به‌ویژه برای کسانی که هیچ هویت یا کارت شناسایی در دولت ندارند. درحالی‌که برخی ازکشورها ممکن است جنگ‌زده باشند، کشورهای دیگری ممکن است حکومت‌هایی داشته باشند که هیچ برنامه‌ای برای ارائه کارت شناسایی به آن‌ها ندارند. شهروندان چنین کشورهایی ممکن است راهی برای ورود به حساب پس‌انداز یا حساب کاربری کارگزاری و در نهایت راهی برای افزایش ثروت خیال راحت نداشته باشند.

موافقان و منتقدان بلاکچین

بلاکچین به‌عنوان یک ابزار غیرمتمرکز برای نگهداری سوابق، تقریباً بدون محدودیت است. از حریم خصوصی بیشتر کاربر و افزایش امنیت گرفته تا کاهش هزینهٔ پردازش و خطاهای کمتر. فناوری بلاکچین ممکن است برنامه‌های کاربردی را بسیار بیشتر از موارد ذکر شده در بالا پوشش دهد؛ بااین‌حال، برخی از معایب نیز وجود دارد.

موافقان

- عدم نیاز به مشارکت انسان جهت تأیید فرایند.
- کاهش هزینه‌ها به‌واسطه حذف مرحله تأیید توسط انسان.

- ایجاد اطمینان تقریبا صددرصدی از عدم مداخله و دست‌کاری به‌واسطه ایجاد تمرکززدایی.
- معاملات ایمن، شخصی و کارا هستند.
- فناوری شفاف.
- فراهم کردن یک روش بانکی و راهی برای حفاظت از اطلاعات خصوصی شهروندان درکشورهایی که دموکراسی نامنظم یا کم‌ارزش دارند.

منتقدان

- مصرف قابل توجه انرژی و آلودگی ناشی از استخراج معادن.
- TPS پایین (معاملات در ثانیه) در مقایسه با VISA و سایر سیستم‌ها.
- سابقه طولانی فعالیت‌های غیرقانونی با استفاده از رمزارزهای موجود مبتنی بر بلاکچین.
- عدم وجود مقررات و نهادهای نظارتی رسمی.

مزایای بلاکچین

دقت زنجیره

شبکه‌ای متشکل از هزاران رایانه (گره) تمام تراکنش‌های موجود در این شبکه را تأیید می‌کند. این تقریباً تمام مشارکت انسان در تأیید فرایند را ریشه‌کن می‌کند، همچنین منجر به کاهش میزان خطای انسانی و یک روند ثبت اطلاعات صحیح می‌شود. اگر یک رایانه در شبکه اشتباهی در ورودی ایجاد کند، این خطا فقط در یک کپی از بلاکچین منعکس می‌شود؛ قبل از اینکه خطا بتواند به بقیه بلاکچین‌ها سرایت کند، باید حداقل توسط ٪۵۱ زنجیره ایجاد شود، که اکثریت شبکه است و این احتمالاً برای یک شبکه بزرگ و در حال رشد از بیت‌کوین غیرممکن است.

زمان کارآمد تسویه معاملات

استقرار معاملات انجام‌شده از طریق یک مرجع مرکزی ممکن است چند روز طول بکشد؛ برای مثال، اگر سعی کنید یک چک را در عصر جمعه واریز کنید، وجوه ممکن است تا صبح روز دوشنبه در حساب شما منعکس نشود. درحالی‌که مؤسسات پنج روز در هفته و در ساعات کاری فعالیت می‌کنند، بلاکچین ۷/۲۴ سالانه و بی‌وقفه کار می‌کند. معاملات را می‌توان طی کمترین زمان مثلاً در ده دقیقه انجام داد و می‌توان تنها پس از چند ساعت آن‌ها را ایمن در نظر گرفت.

معاملات خصوصی

بسیاری از شبکه‌های بلاکچین به‌عنوان پایگاه‌های داده عمومی فعالیت می‌کنند. این بدان معنی است که هرکسی اتصال اینترنتی قوی داشته باشد، می‌تواند فهرستی از تاریخچه معاملات شبکه را مشاهده کند. اگرچه کاربران می‌توانند جزئیات مربوط به معاملات صورت گرفته را بررسی کنند، همین‌طور آن‌ها می‌توانند اطلاعات مربوط به کاربرانی را مشخص کنند که از معاملات آن‌ها استفاده می‌کنند. فرض اینکه شبکه‌های بلاکچین مانند بیت‌کوین ناشناس و محرمانه و ایمن است، معمول است.

این بدان معناست که وقتی کاربر مبادله‌ای را در انظار عمومی انجام می دهد، یک کد به‌جای اطلاعات شخصی آن‌ها در بیت‌کوین ثبت می‌شود. اگر شخص بیت‌کوین را در صرافی خریداری کرده باشد که نیاز به شناسایی دارد، سپس هویت شخص هنوز با همان کد در آدرس بلاکچین مرتبط است؛ بنابراین یک معامله، حتی اگر به نام یک شخص باشد، هیچ اطلاعات شخصی را درباره او فاش نمی‌کند.

معایب بلاکچین

اگرچه بلاکچین دستاوردهای عمده‌ای دارد؛ اما چالش‌های پذیرش بلاکچین و مشکلات و موانع استفاده از آن فقط محدود به موارد فنی نیست. چالش‌های واقعی سیاسی و نظارتی، مهم‌تر از ذکر هزاران ساعت طراحی نرم‌افزار سفارشی و برنامه‌نویسی مورد نیاز برای ترکیب بلاکچین در شبکه‌های تجاری است. در اینجا برخی از این چالش‌ها ذکر شده است:

هزینه فناوری

اگرچه وجود بلاکچین باعث صرفه‌جویی در هزینه‌های معاملات کاربر می‌شود، اما فناوری آن کاملاً رایگان نیست. الگوریتم و سیستم «اثبات کار» بیت‌کوین برای تأیید معاملات از مقدار زیادی محاسبات استفاده می‌کند. در دنیای فیزیکی، توان مصرفی برای این مقدار محاسبه توسط میلیون‌ها رایانه در شبکه بیت‌کوین، نزدیک به مصرف سالانهٔ کشور دانمارک است.

صرف‌نظر از هزینه‌های استخراج بیت‌کوین، کاربران همچنین برای تأیید معاملات در بلاکچین، مصرف برق خود را افزایش می‌دهند. وقتی ماینرها شامل یک بلوک از یک بلاکچین می‌شوند، باید بیت‌کوین کافی برای محاسبه زمان و انرژی داشته باشند. برای بلاکچین‌هایی

که از رمزارز استفاده نمی‌کنند، ماینرها مایلند به آن‌ها پرداخت شود یا در غیر این صورت تشویق می‌شوند معاملات را تأیید کنند. راه‌حل‌های خاصی برای این مسائل شروع شده است؛ به‌عنوان مثال، بیت‌کوین مزارع استخراج بیت‌کوین به‌گونه‌ای طراحی می‌شوند که از انرژی خورشیدی، گاز طبیعی اضافی تأسیسات، یا نیروگاه‌های بادی استفاده کنند. این امر می‌تواند با کاهش مصرف برق جهت استخراج همراه باشد.

ناکارآمدی سرعت

بیت‌کوین بهترین نمونه از ناکارآمدی‌های احتمالی بلاکچین است. سیستم Bitcoin's "PoW" (اثبات کار) حدود ده دقیقه طول می‌کشد تا بلوک جدید ایجاد کند؛ بنابراین محاسبه شده است که با این سرعت، بلاکچین فقط می‌تواند از حدود هفت تراکنش در ثانیه مراقبت کند (TPS). گرچه رمزارزهای دیگر مانند "Ethereum" عملکرد بهتری نسبت به بیت‌کوین دارند، آن‌ها هنوز توسط بلاکچین محدود شده‌اند. مثلاً سیستم‌های قدیمی ویزا، می‌تواند حداکثر ۲۴۰۰۰ TPS را پردازش کند.

راه‌حل‌های این مشکل سال‌هاست که در دست توسعه است. در حال حاضر، برخی از بلاکچین‌ها بیش از ۳۰،۰۰۰ تراکنش در ثانیه پردازش می‌کنند.

فعالیت‌های غیرقانونی

در شبکه بلاکچین کاربران در برابر هک و حریم خصوصی محافظت می‌شوند؛ بااین‌حال، شبکه بلاکچین فرصتی برای تجارت و فعالیت غیرقانونی در بازار ایجاد می‌کند. نمونهٔ بارز استفاده از بلاکچین برای مبادلات غیرقانونی، جاده ابریشم است. یک شبکه توزیع داروی آنلاین به نام «وب تاریک» که از فوریه ۲۰۱۱ تا اکتبر ۲۰۱۳ فعالیت می‌کرد و FBI آن را متوقف کرد.

این وب‌سایت به کاربران امکان می‌دهد که با استفاده از مرورگر Tor، بدون اینکه دنباله‌ای در وب‌سایت داشته باشند به مرور آن بپردازند و خریدهای غیرقانونی در بیت‌کوین یا سایر رمزارزها انجام دهند. قوانین کنونی ایالات متحده به ارائه‌دهندگان خدمات مالی نیاز دارند که هنگام ثبت‌نام مشتریان، هویت هر مشتری را بررسی کنند تا اطمینان حاصل شود که مشتری در هیچ‌یک از فهرست‌های گروه‌های تروریستی نیست. این می‌تواند مزایا و معایبی داشته باشد، بیشتر به این دلیل که به هرکسی امکان دسترسی به حساب‌های مالی را می‌دهد و اجازه می‌دهد تا مجرمان به مبادلات خود ادامه دهند. گرچه مردم بحث کرده‌اند که استفاده خوب از

رمزنگاری، مانند بانکداری در جهان بدون بانک، بیش از استفاده بد از آن رایج است؛ به‌ویژه هنگامی که بسیاری از فعالیت‌های غیرقانونی که هنوز هم ادامه دارد از طریق پول نقد غیرقابل ردیابی و ارزهای فیات انجام می‌شود.

فصل ۳

معرفی قراردادهای هوشمند

«قراردادهای هوشمند تضمین‌کننده مجموعه نتایج ویژه هستند. سردرگمی و نیاز به دادخواهی وجود ندارد» (جف گارزیک[1] صاحب خدمات بلاکچین با نام بلاک[2]).

قراردادهای هوشمند برنامه‌هایی هستند که روی بلاکچین اتریوم[3] اجرا می‌شوند. آن‌ها، مجموعه‌ای از کدها (توابع) و داده‌ها (وضعیت) هستند که در یک نشانی بلاکچین اتریوم مخصوص قرار دارند.

قراردادهای هوشمند نوعی حساب اتریوم است. به عبارت دیگر، شامل تراز وجوه بوده و می‌تواند معاملات را در سراسر شبکه فعال کند. البته، این نوع قراردادها توسط هیچ‌یک از اعضای شبکه قابل کنترل نیستند. بلکه در سراسر شبکه برنامه‌ریزی و توزیع شده و با روشی کار می‌کند که از پیش تنظیم یا رمزگذاری شده است. حساب‌های کاربری با ارسال تراکنش‌هایی که عملکرد غیرمتمرکز دارند با قراردادهای هوشمند ارتباط برقرار می‌کنند.

قراردادهای هوشمند قوانینی را به‌عنوان قراردادهای عادی مشخص می‌کنند و این قوانین با استفاده از کد، به‌طور خودکار اجرا می‌شوند. قراردادهای هوشمند بدون هرگونه واسطه‌ای تبادل پول، دارایی، سهام یا هر چیز ارزشمندی را به روش شفاف و بدون تعارض آسان می‌کنند. خروجی خاص با ورودی صحیح همخوانی دارد. این منطق به همان روشی که در یک قرارداد هوشمند رمزگذری شده است، در دستگاه فروش نیز کدگذاری می‌شود.

هرکسی می‌تواند قراردادهای هوشمند را امضا کرده و از آن‌ها در وب استفاده کند. تنها

---

1. Jeff Garzik
2. BLOQ
3. Ethereum

کدنویسی به زبان هوشمند مورد نیاز بوده و اتریوم کافی برای استفاده از قرارداد را باید داشته باشید. استفاده از یک قرارداد هوشمند از نظر فنی همانند یک معامله است؛ یعنی هزینه گاز را به همان روشی پرداخت کنید که یک انتقال ساده اتریوم صورت می‌گیرد. گرچه هزینه گاز استفاده از قرارداد بسیار بیشتر است.

اتریوم برای نوشتن قراردادهای هوشمند یک زبان رمزگذار مناسب به نام «سالیدیتی[1]» را ارائه می‌دهد.

سالیدیتی، یک زبان برنامه‌نویسی شیءگرا است برای نوشتن قراردادهای هوشمند. نکته قابل توجه در مورد اتریوم این است که می‌توان قراردادهای هوشمند را به زبان ساده گسترش داد. اگر تجربه استفاده از پایثون[2] یا جاوا اسکریپت[3]را دارید، به‌راحتی قادر خواهید بود تا یک قرارداد هوشمند با چهارچوب مناسب ایجاد کنید.

قراردادهای هوشمند عملکرد کاربران را در بستر اتریوم برنامه‌ریزی می‌کنند. سالیدیتی از پایثون و سی پلاس پلاس[4] و جاوا اسکریپت الهام گرفته شده و برای برنامه‌های مجازی اتریوم ساخته شده است. از آن بیشتر برای انجام قراردادهای هوشمند در سیستم عامل‌های مختلف بلاکچین مانند اتریوم استفاده می‌شود. این برنامه توسط آتکس بگساگسازی[5] و کرستین رایتویسنر[6] و گروهی از توسعه‌دهندگان اصلی اتریوم برای ایجاد قراردادهای هوشمند در سیستم عامل‌های بلاکچین ساخته شده است. زبان برنامه‌نویسی سالیدیتی در درجهٔ نخست برای توسعه کد و پیاده‌سازی برنامه مجازی اتریوم در نظر گرفته شده است. علاوه بر این، قراردادهای هوشمند همانند سایر قراردادهای متعارف قوانین و مقررات خود را دارند و این تعهدات را به‌طور خودکار اجرا می‌کنند.

وایپر[7]

وایپر به شما این امکان را می‌دهد تا روی اتریوم برنامه‌نویسی کنید. این زبان برنامه‌نویسی پس

---

1. Solidity

توضیح مترجم: زبان برنامه‌نویسی مورد استفاده اتریوم برای توسعه قراردادهای هوشمند است.

2. Python
3. Javascript
4. C++
5. Atex Begsgsazi
6. Christian Reitwissner
7. Vyper

از سالیدیتی برای اتریوم توسعه یافت تا فرایندهای ناامن را محدود و درصد خوانایی را بهبود بخشد. وایپر امنیت و ممیزی قراردادهای هوشمند را به‌طور کامل اجرا می‌کند.

وایپر یک زبان برنامه‌نویسی تجربی و قراردادی است که مانند پایثون به‌صورت ایستا نوشته شده است. مانند اشیای موجود در برنامه‌نویسی شیءگرا[1] هر قرارداد دارای متغیرهای حالت، توابع و انواع داده‌های مشابه است. ویژگی های خاص قرارداد، اطلاع رسانی رویدادها به شنوندگان، متغیرهای جهانی خاص و اجزا ثابت جهانی است.

برخی از نمونه‌های قرارداد اتریوم شامل تأمین مالی جمعی[2]، رأی‌دادن و مزایده است؛ با این‌همه، باید قبل از استفاده گردآوری شود تا ماشین مجازی اتریوم[3] بتواند قرارداد را استنباط و ذخیره کند. قرادادهای هوشمند به‌صورت کلی در اتریوم برای عموم در دسترس است و می‌تواند یک رابط برنامه‌نویسی اپلیکشن[4] باز محسوب شود. این بدان معناست که قراردادهای هوشمند با سایر قراردادهای هوشمند در تماس هستند تا عملکرد خود را گسترش دهند. قراردادها همچنین می‌توانند سایر قراردادها را فعال سازند.

به‌خودیِ‌خود، قراردادهای هوشمند نمی‌توانند درخواست‌های‌ی از جنس «قرارداد انتقال ابر متن[5]» را ارسال کنند؛ بنابراین آن‌ها نمی‌توانند اطلاعات رویداد «واقعی» را بپذیرند. این امر تعمدی است، زیرا استفاده از اطلاعات خارجی می‌تواند اجماع (سازگاری) مهم برای امنیت و تمرکززدایی را از بین ببرد.

روند کار یک قرارداد هوشمند

قرارداد هوشمند یک کد رایانه‌ای خودکار برای اجرای تمام یا بخشی از قرارداد است؛ و معمولاً در بستری ذخیره می‌شود که روی بلاکچین ساخته شده است. چنین کدی فقط ممکن است نشان‌دهندهٔ قراردادی بین طرفین باشد، یا ممکن است برای حمایت از قرارداد متنی استاندارد و مطابقت با مفاد خاص، مانند انتقال وجوه از یک طرف به طرف دیگر استفاده شود.

بنابراین گره‌های چند بلاکچینی می‌توانند از دوام، امنیت و ماهیت تغییرناپذیر بلاکچین بهره‌مند شوند. این مدل نشان می‌دهد که کد هنگامی اجرایی می‌گردد که یک بلوک جدید

1. Object-oriented Programming (OOP)
2. Crowdfunding
3. Ethereum Virtual Machine
4. Application Programming Interface (API)
5. HTTP

به سایر بلوک‌ها یا زنجیره‌های بلوک افزوده شود. در ابتدای معامله اگر اشخاص شرکت‌کننده نشان دهند که پارامترهای خاصی را برآورده می‌کنند، کد به‌طور خودکار عملیاتی را انجام می‌دهد که توسط این پارامترها آغاز شده است.

کد فقط در صورت شروع معامله این کار را انجام می‌دهد. کد تا زمانی‌که معامله‌ها شروع یا فعال نشود هیچ‌کاری انجام نخواهد داد. بیشتر قراردادهای هوشمند با استفاده از یک زبان برنامه‌نویسی، مشابه بسیاری از زبان‌های برنامه‌نویسی پرکاربرد، برای برنامه‌های رایانه‌ای مانند سالیدیتی کدگذاری می‌شوند.

در حال حاضر، عوامل و شاخص‌های تأییدکننده قراردادهای هوشمند باید مشخص شود. آن‌ها همچنین باید به‌صورت اهداف عینی تعیین شوند؛ یعنی اگر حالت «الف» اتفاق افتاد، آنگاه مرحله «ب» را دنبال کنید. بنابراین کار واقعی یک قرارداد هوشمند، یک کار اساسی است: مانند انتقال عادی ارزهای رمز پایه از کیف پول یک شخص به کیف پول دیگری بر اساس معیارهای خاص. با رشد و ساده‌سازی بلاکچین یا افزایش دارایی‌های منتقل شده به زنجیره، قراردادهای هوشمند پیچیده‌تر می‌شوند و معاملات پیچیده‌تری انجام می‌دهند.

در حال حاضر، توسعه‌دهندگان در روند معامله برای ایجاد قراردادهای هوشمند پیشرفته‌تر، چندین مرحله را ترکیب می‌کنند؛ بااین‌حال، حداقل چند سال طول می‌کشد تا کد مورد نظر بتواند استانداردهای حقوقی ذهنی بیشتری را تعریف کند؛ مانند انطباق با استانداردهای عملیاتی تجاری رایج یا نیاز به مقررات جبران خسارت. هم‌اکنون بسیاری از شرکت‌های حقوقی، توسعه‌دهندگان را استخدام می‌کنند تا بتوانند در دوره جدید قراردادهای پیمانکاری شرکت کنند.

پیش از اینکه قراردادهای هوشمند در بلاکچین اجرا شود، پرداخت هزینه‌های اجرای قراردادها ضروری است. برای مثال اگر قرار است یک قرارداد هوشمند در بلاکچین اتریوم اجرا شود، مراحل قرارداد معمولاً در ماشین مجازی اتریوم انجام می‌شود و طرفین قرارداد با استفاده از سکهٔ رمزنگاری اتریوم به نام «گاز[1]» یا «ای‌ثر[2]» هزینهٔ معاملات را پرداخت می‌کنند. هرچه قراردادهای هوشمند پیچیده‌تر باشند، بسته به مراحل معامله، مقدار گاز پرداختی برای تحقق قراردادهای هوشمند بیشتر خواهد بود؛ بنابراین، در حال حاضر گاز یک درگاه یا ورودی مهم برای جلوگیری از ازدحام ماشین مجازیِ اتریوم با قراردادهای بسیار پیچیده یا چندگانه است.

قراردادهای هوشمند برای انجام دو نوع معامله بسیار مناسب هستند. اولین مورد، اطمینان

1. Gas
2. Ether

از پرداخت پول در شرایط خاص است و دوم، اعمال شرایط جدید مالی در صورتی که مفاد قرارداد اجرا نگردد. در هریک از این دو مورد، به‌محض اینکه قراردادهای هوشمند مستقر و کار آغاز شد، هیچ مداخلهٔ انسانی یا قضایی لازم نیست. این موضوع هزینهٔ عملیاتی و اجرایی قرارداد را به حداقل می‌رساند.

برای نمونه، قراردادهای هوشمند می‌توانند برخی از الزامات و تشریفات قراردادها مانند «پرداخت در برابر دریافت» را برطرف کنند. اگر محموله‌ای به انبار رسیده و مراحل اسکن مورد نیاز را طی کند، قرارداد هوشمند بلافاصله درخواست مجوز لازم را صادر می‌کند و پس از دریافت می‌تواند بلافاصله پول را از خریدار به فروشنده منتقل نماید.

فروشنده سریع‌تر پرداخت‌های خود را دریافت می‌کند، دیگر نیاز به پیگیری پرداخت نیست و همچنین خریدار، هزینهٔ پرداخت را به حداقل می‌رساند. این می‌تواند نیاز سرمایه در گردش را تحت‌تأثیر قرار داده و معاملات مالی را برای دو طرف معامله ساده کند. پس از اجرایی شدن، قراردادهای هوشمند می‌توانند رمزگذاری‌شده تا در صورت عدم پرداخت، دسترسی به دارایی مبتنی بر اینترنت را غیرفعال کنند؛ به‌عنوان مثال اگر پرداختی انجام نگیرد دستیابی به محتوای خاص ممکن است به‌طور خودکار غیرفعال شود.

ویتالیک بوترین[1] برنامه‌نویس ۲۷ ساله اتریوم، قرارداد هوشمند را چنین شرح می‌دهد: در سیستم قرارداد هوشمند، یک دارایی یا ارز به برنامه‌ای منتقل می‌شود که کد مورد نظر را اجرا می‌کند و در برخی موارد به‌طور خودکار، یک شرط را تأیید و یا تعیین می‌کند که آیا دارایی باید به شخص x منتقل گردد یا به شخص y برگردد، یا باید فوراً به شخص ارسال‌کننده یا ترکیبی از هر دو منتقل شود.

دفتر غیر متمرکز[2] نیز سند را نگهداری و کپی می‌کند که به آن امنیت و تغییرناپذیری خاصی می‌دهد؛ برای مثال، اگر آپارتمانی را از شخصی اجاره کنید، می‌توانید این کار را با پرداخت رمزارز از طریق بلاکچین انجام دهید و سپس رسید مجازی خود را از صاحبخانه دریافت و نگهداری کنید. وی در عوض، کلید ورود دیجیتال را در یک تاریخ خاص به شما می‌دهد.

فرض کنید کلید به‌موقع تحویل داده نشود، در این صورت بلاکچین دستور بازپرداخت را می‌دهد. بااین‌حال، اگر کلید قبل از تاریخ اجاره ارسال شود، این موضوع ثبت شده و هنگام سررسید، کلید و هزینه به ترتیب، به شما و صاحب‌خانه تحویل داده می‌شود.

---

1. Vitalik Buterin
2. Decentralized Ledger

این سیستم بر پایهٔ اصل «درصورتی که[1]» کار می‌کند و اغلب صدها نفر شاهد آن هستند؛ بنابراین می‌توانید اطمینان داشته باشید که تمامی مفاد قرارداد به‌صورت کامل اجرا می‌شود. اگر صاحب‌خانه کلید را به شما بدهد، مطمئناً به او پول پرداخت می‌شود. اگر مبلغ را به ارز بیت‌کوین پرداخت کنید آنگاه کلید را دریافت خواهید کرد. وگرنه سند پس از گذشت زمان مورد نظر فوری لغو می‌شود. گرچه بدون اطلاع هر دوی شما، کد مورد نظر لغو نمی‌شود چون همهٔ طرفینِ قرارداد باید از هرگونه اقدامی مطلع باشند. شما می‌توانید از قراردادهای هوشمند برای هر موقعیتی اعم از مشتقات مالی، لغو قرارداد، خدمات مالی، حق بیمه، املاک، اعتباردهی، فرایندهای قانونی تا توافق‌نامه‌های تأمین مالی استفاده کنید.

چگونه می‌توانید از قراردادهای هوشمند استفاده کنید؟

بنا به گفتهٔ جری کومو[2]، معاون فناوری بلاکچین در شرکت آی.بی.ام[3]:«قراردادهای هوشمند را می‌توان در همهٔ زمینه‌ها از جمله خدمات مالی، بهداشت و درمان، بیمه و غیره استفاده کرد». در اینجا روش‌هایی برای استفاده از قراردادهای هوشمند وجود دارد:

دولت

با استفاده از قراردادهای هوشمند، شهروندان دیگر نگران تقلب در آرای خود نیستند؛ زیرا با ایجاد یک سیستم ماندگار، ضد تقلب و ایمن تمام نگرانی‌ها برطرف می‌شود. آرای محافظت شده باید رمزگشایی شوند و برای دستیابی به آن‌ها به قدرت محاسباتی زیادی نیاز است؛ اما از جایی که هیچ‌کس قدرت محاسباتی لازم را به‌طور کامل ندارد، بنابراین برای هک یا نفوذ به سیستم به قدرت محاسباتی خداگونه‌ای نیاز است.

همچنین، قراردادهای هوشمند می‌توانند میزان پایین مشارکت رأی‌دهندگان را افزایش دهند. بسیاری از بی‌تحرکی‌ها از یک سیستم نامتعادل ناشی می‌شود که شامل صف، نمایش هویت و پُر کردن فرم است. داوطلبان حتی می‌توانند رأی‌گیری آنلاین انجام دهند و آن‌گاه میزان مشارکت‌کنندگان افزایش می‌یابد.

1. If-then
2. Jerry Cuomo
3. IBM

مدیریت

قراردادهای هوشمند ارائه‌شده توسط بلاکچین نه‌تنها به‌عنوان یک منبع (دفتر کل) مورد اعتماد است، بلکه به‌علت دقت و شفافیت و سیستم خودمختار، در گردش کار و ارتباطات هم مورد استفاده قرار می‌گیرد. پس از مرتب‌سازی ورودی و خروجی داده‌های معاملات تجاری، آن‌ها می‌باید با قوانین منطبق باشند؛ اما قراردادهای هوشمند بلاکچین با بهینه‌سازی امور و با رویهٔ مستقل، هرگونه هزینهٔ اضافی و مشکلات حقوقی ناشی از قراردادها، همانند تأخیر در تسویه‌حساب را از بین می‌برند.

صنعت خودرو

در این موضوع شکی نیست که ما به‌سرعت در حال تبدیل شدن به روبات‌های هوشمند هستیم. اگر به آینده فکر کنیم خواهیم دید آنجا همه چیز خودکار است؛ گوشی‌ها هوشمند، عینک هوشمند و حتی ماشین‌ها هوشمند هستند و بی‌گمان جایی است که قراردادهای هوشمند به ما کمک خواهد کرد. برای مثال، می‌خواهیم در مورد وسایل خودکار یا خودروهایی با توانایی پارک خودکار صحبت کنیم. قراردادهای هوشمند همانند یک پیشگو عمل می‌کنند به‌گونه‌ای که در مورد علت تصادفات رانندگی، راننده، حس‌گرها یا سایر بخش‌های وسیله نقلیه به ما اطلاعات می‌دهند.

با کمک قراردادهای هوشمند شرکت‌های ارائه‌دهندهٔ خدمات بیمه خودرو، بر اساس اینکه مشتریان در چه شرایطی از خودرو خود استفاده می‌کنند، مبلغ خسارت را محاسبه و پرداخت می‌کنند.

املاک

از طریق قراردادهای هوشمند پول خیلی زیادی به دست می‌آید. مراحل جاری زیر برای کسی که می‌خواهد یک آپارتمان را اجاره بدهد انجام می‌شود. شما باید به‌طور متوسط مبلغی را به آژانس تبلیغات یا روزنامه پرداخت کنید و دوباره هزینهٔ دیگری برای پیگیری در خصوص پرداخت کرایه. درحالی‌که با قراردادهای هوشمند هزینه‌های شما کاهش پیدا می‌کند و تمام کاری که باید انجام بدهید پرداخت بیت‌کوین و رمزگذاری قرارداد خود، در دفتر کل است. خیلی سریع به آن چیزی می‌رسید که می‌خواهید (آگهی شما را همه می‌بینند) و کارگزاران، دلالان، وام‌دهندگان و همهٔ آن‌هایی که در این موضوع دخیل هستند سود خود را به دست می‌آورند.

بخش سلامت

پرونده پزشکی هر فرد می‌تواند بر اساس بلاکچین به‌صورت ارائه فرم‌های خصوصی کاملاً محرمانه طبقه‌بندی و رمزگذاری شود که از قبل تکمیل شده است؛ این روش بر اساس قوانین ایمن و محرمانهٔ «قانون انتقال و پاسخ‌گویی الکترونیک بیمه سلامت[1]» انجام شده و می‌توانیم به آن اطمینان کنیم.

علاوه بر این، پرونده‌های جراحی در بلاکچین قابل بایگانی‌اند و به‌طور خودکار به ارائه‌دهندگان خدمات درمانی و بیمه، به‌عنوان مدارک لازم تحویل داده می‌شوند. همچنین از دفتر کل برای مدیریت مراقبت‌های سلامت عمومی مانند نظارت بر درمان‌ها (تجویزها)، تنظیم اطلاعات، نتیجه آزمایش و ساماندهی کیفیتِ مراقبت‌های پزشکی می‌توان استفاده کرد.

فواید قرارداد های هوشمند

قراردادهای هوشمند یک ویژگی متمایزکنندهٔ اتریوم و سایر رمزارزها از ارزهای رایج[2] هستند. در اینجا به چند ویژگی مهم قراردهای هوشمند اشاره می‌کنیم:

استقلال

تحت یکسری شرایط که با آن‌ها توافق می‌کنید، شما دیگر نیازی به وجود کارگزار واسط، حقوقدان یا هر واسطهٔ دیگری برای تأییدیه ندارید که همین امر سبب می‌شود خطرات ناشی از دست‌کاری توسط شخص ثالث (واسطه) کاهش یابد.

از جایی که این کار توسط شبکه هوشمند به‌جای استفاده از یک فرد یا افرادی انجام می‌شود که ممکن است ندانسته اشتباه کنند، پس منافع شما کاملاً تضمین و محفوظ شده باقی می‌ماند.

اعتماد

داده‌ها و فایل‌های شما روی یک دفتر کل مشترک رمزگذاری‌شده باقی می‌ماند که ریسک ناشی از فاش یا گم شدن اطلاعات شما توسط دیگران از بین می‌رود و شما اطمینان خواهید داشت هر زمانی که بخواهید به اطلاعات‌تان دست خواهید یافت.

پشتیبانی

این احتمال هست که بانک شما، اطلاعات حساب شما را از دست بدهد. ولی این موضوع در بلاکچین اصلاً مطرح نیست. در بلاکچین تمام دوستان‌تان، نسخهٔ پشتیبانی از اطلاعات دارند.

---

1. HIPAA
2. Fiat currencies

اطلاعات شما به دفعات زیاد در جاهای مختلف کپی شده است و همواره نسخهٔ دیگری از اطلاعات شما وجود خواهد داشت.

امنیت

اطلاعات شما با رمزنگاری و وب‌سایت‌های رمزگذاری کاملاً ایمن هستند و نیازی برای نگرانی در خصوص اطلاعات خود نباید داشته باشید.

هک کردن اطلاعات نیاز به یک استعداد خاص دارد؛ هکرها باید با رمزگشایی کدها به اطلاعات شما نفوذ کنند که سریعاً این الگوریتم به نسخه بعدی ارتقا پیدا می‌کند.

سرعت

پردازش دستی داده‌ها بسیار زمان‌بر است و نیاز به کاغذبازی زیادی دارد، اما قراردادهای هوشمند با استفاده از کدهای نرم‌افزاری، امضای خودکار انجام می‌دهند؛ بنابراین زمان کمتری برای پردازش کسب‌وکار یا سایر مستندسازی‌ها صرف می‌کنند.

پس‌انداز

شما ممکن است به یک واسط یا کارگزار برای کنترل معامله هزینه پرداخت کنید؛ اما قراردادهای هوشمند واسطه‌ها را معاف می‌کند و هزینه شما پس‌انداز می‌شود.

دقت

قراردادهای هوشمند رایانه‌ای بابت سرعت و ارزانی‌شان شناخته شده‌اند و قابلیت عدم خطا در تکمیل فرم‌ها؛ بنابراین خطایی پیش نمی‌آید یا به‌طور فوق‌العاده‌ای کم است.

معایب قراردادهای هوشمند

قراردادهای هوشمند برای کسب‌وکار و فن‌آوریِ بلاکچین، همچون لاستیک برای پیمودن مسیر و جاده هستند. درحالی‌که فقط چند مورد کسب‌وکار از سرویس توزیع تخصصی مالی استفاده می‌کردند، بلاکچین پدیدار شد؛ برای مثال: خدمات دفتر کل پرداخت در بورس اوراق بهادار «یانگون[1]» میانمار. این خدمات بلاکچین خیلی جذاب هستند. هستهٔ معاملات بورس اوراق بهادار «یانگون» در طول روز معاملات را دو بار به‌روزرسانی می‌کند و از تسویه معاملات توزیع‌شده[2] استفاده می‌کند. اما ظرفیت‌های اجرایی خودکار قراردادهای هوشمند، میزان اطمینان از امنیت معاملات را در شرایط پیچیده ارتقا می‌دهند تا جایی که نیازمند تغییر عمیق[3] معاملات

1. Yangoon Stock Exchange
2. Distributed settlement
3. Context Transition

است. و این موضوع همان احتمالی است که شرکت‌های آمازون، ماکروسافت، آزور، آی.بی.ام بلاکچین را به‌عنوان یک سرویس[1] گسترش دادند.

قراردادهای هوشمند گرچه خیلی جذاب و شگفت‌انگیز به نظر می‌رسند، ولی کامل نیستند. برای مثال، نقص نرم‌افزار می‌تواند مشکل حاد و جدی ایجاد کند. دولت‌ها در نحوه تنظیم و نظارت بر قراردادهای هوشمند دچار چالش هستند و یا نمی‌توانند بر آن‌ها مالیات وضع کنند. حتی ممکن است مشکل ارسال اشتباهِ کد وجود داشته باشد، همانند موضوع اجاره‌ای که پیش‌تر صحبت کردیم. بعضی اوقات هم ممکن است ارسال کد به‌درستی انجام گیرد، ولی آپارتمان، بدون اجازه شما و پیش از موعد سررسید اجاره، کاربری عمومی پیدا کند.

در پردازش فرایند قراردادها اینکه چه اتفاقی افتاده خیلی اهمیتی ندارد. چالش‌های قرارداد هوشمند تا وقتی که به آن فکر کنید وجود دارد. گرچه کارشناسان می‌کوشند تا این موارد را حل کنند؛ اما برای کسانی که به این قراردادهای هوشمند امیدوارند، این موارد دلسردکننده به نظر می‌رسد.

بلاکچین بستری است که پردازش قراردادهای هوشمند از آن عبور می‌کند:

بیت‌کوین: برای انجام معاملات از بیت‌کوین استفاده می‌کنند، گرچه قابلیت محدودی در پردازش داده‌های قرارداد هوشمند دارد.

زنجیره جانبی[2]: نام دیگر بلاکچین است که به موازات بلاکچین اجرا می‌شود و طیف گسترده‌تری برای پردازش قراردادهای هوشمند نسبت به بیت‌کوین دارد.

ان. ایکس. تی[3]

یک مجمع رایج بلاکچین که برای انتخاب محدودی از قالب‌های قراردادهای هوشمند است. شما مجبور به استفاده از منابع در دسترس هستید؛ زیرا کدهای مستقل از این منابع در دسترس نیست. اتریوم نوع رایج و شناخته‌شده از مدل بلاکچین که برای رمزگذاری و پردازش قراردادهای هوشمند، پیشرفته‌تر است. در این مدل شما در انتخاب کدها آزادی عمل بیشتری دارید؛ اما برای محاسبات قوی باید با توکن‌های ای.تی.اچ[4] پرداخت را انجام دهید.

قراردادهای هوشمند با توجه به تعداد صنایعی که می‌توانند بر آن تأثیرگذار باشند، نامحدود هستند. برای مثال، بخش سلامت، املاک و حتی مسائل حقوقی. فهرست قابلیت‌ها و ظرفیت‌های آن بسیار زیاد است.

---

1. Blockchain as a Service (BaaS)
2. Side chains
3. NXT
4. ETH

فصل ۴

اتریوم و نظام مالی غیرمتمرکز

بیایید با این فرض شروع کنیم که اکثر پروژه‌های نظام مالی غیرمتمرکز روی اتریوم ساخته شده‌اند.

اتریوم یک بلاکچین غیرمتمرکز است که به سایر برنامه‌های غیرمتمرکز زنجیره بلوک[1] اجازه می‌دهد تا بر اساس قراردادهای هوشمند ساخته شوند. برخی از این برنامه‌ها می‌توانند رمزهای ارز خود را (توکن‌های قابل تعویض) داشته باشند. این ترکیب یکی از پروتکل‌هایی است که بیشتر با خدمات مالی غیرمتمرکز مربوط به پس‌انداز و وام سروکار دارد.

دلیل اصلی این امر بسترهای قدرتمند قرارداد هوشمند اتریوم است. این بسترها به شما اجازه می‌دهند تا قراردادهای هوشمند پیشرفته را بنویسید که حاوی تمامی منطق برنامه نظام مالی غیرمتمرکز است. علاوه بر این، اتریوم، دارای پیشرفته‌ترین اکوسیستم برای همهٔ بسترهای قرارداد هوشمند است. هزاران توسعه‌دهنده هر روز برنامه‌های کاربردی جدیدی ایجاد می‌کنند ولی بیشترین ارزش در قراردادهای هوشمندی است که اثرات شبکه‌سازی بیشتری به دست دهد.

زبان سالیدیتی یکی از زبان‌های برنامه‌نویسی است که به‌طور گسترده در قراردادهای هوشمند موجود در بلاکچین اتریوم مورد استفاده قرار می‌گیرد. این زبان امکان ایجاد قراردادهای پیشرفته هوشمند را فراهم می‌کند که شامل تمام منطق لازم برای برنامه‌های کاربردی نظام مالی غیرمتمرکز است. همچنین، اتریوم در میان سیستم‌عامل‌های قرارداد هوشمند، پیشرفته‌ترین سیستم را دارد؛ با در نظر گرفتن تعدادِ فزایندهٔ توسعه‌دهندگانی که در

1. dApps

حال گسترش برنامهٔ جدید هستند و هر روز اپلیکیشن‌های جدیدی ابداع می‌کنند؛ در نتیجه اثرات شبکه‌سازی بیشتری ایجاد می‌شود.

بستر قراردادهای هوشمند اتریوم، فضای بیشتری برای انعطاف‌پذیری می‌دهد و در صورت تحقق شرایط، معاملات را سریع انجام می‌دهد. زبان‌های برنامه‌نویسی قراردادهای هوشمند اتریوم مانند سالیدیتی، برای توسعه و استقرار قراردادهای هوشمند ایجاد می‌شوند. برای مثال، اگر کاربری بخواهد پول خود را برای دوست خود در یک پنج‌شنبه انتقال دهد، فقط کافی‌ست دمای هوا مطابق با سایت آب‌وهوا[1] به ۸۵ درجه فارنهایت برسد. مثال دیگر تغییر اجاره زمین‌های کشاورزی شما بر اساس قیمت‌های آتی ذرت است (یعنی اوراق بهادار قرارداد آتی). قوانین و بندهایی از این دست می‌تواند در یک قرارداد هوشمند گنجانده شود. بسیاری از برنامه‌های نظام مالی غیرمتمرکز در اتریوم با قراردادهای هوشمند به‌طور متمرکز اجرا می‌شوند.

برنامه‌های محبوب نظام مالی غیرمتمرکز: وام‌دهی و وام‌گیری

میکردائو

میکردائو[2] (سازمان مستقل غیرمتمرکز) یکی از پروژه‌های اصلی در مراحل نخست نظام مالی غیرمتمرکز بود. این پروژه در سال ۲۰۱۵ شروع شد و به کاربران اجازه تولید دای (یعنی رمزارز) را داد. دای اولین ارز پشتیبانی‌شدهٔ خنثی در جهان و یک کوین پایدار غیرمتمرکز پیشرو بود. همچنین به کاربران امکان می‌داد تا برای اخذ تسهیلات، وثیقه بگذارند. دای، یک کوین ثابت است که قیمت‌ها را به دلار آمریکا کشف می‌کند.

همچنین برای صرفه‌جویی در هزینه‌ها در سیستم عامل میکردائو می‌توان از دای استفاده کرد. همچنین برای اخذ وام که یکی از موضوعات اصلی نظام مالی است. نظام مالی غیرمتمرکز در تلاش است یک اکوسیستم اقتصادی کاملاً جدید ایجاد کند که به مجوز نیاز ندارد و شفاف است. وام یا سهام، بخشی از این اکوسیستم است. سایر ویژگی‌ها شامل کوین‌های ثابت، مبادلات غیرمتمرکز، مشتقات، معاملات حاشیه‌ای و بیمه هستند.

دای یک رمزارز پایدار[3] است که سعی می‌کند با بهره‌گیری از یک سیستم قرارداد هوشمند خودکار روی سیستم‌عامل اتریوم، ارزش خود را در نزدیکی ارزش دلار آمریکا حفظ کند. دای

1. www.weather.com
2. MakerDAO
3. Stable crypto coin

پایدار است و تحت ساختار حاکمیت میکردائو فعالیت می‌کند. میکردائو یک سازمان خودمختار دیکس (یعنی صرافی غیرمتمرکز) است، متشکل از دارندگان بلیط کنترل‌شده توسط میکر (ارز دیجیتال)[1] و می‌تواند در مورد تغییر در پارامترهای خاص قراردادهای هوشمند برای پایدار نگه داشتن دای، رأی دهد. سیستم‌های دای و میکردائو به‌عنوان نظام مالی غیرمتمرکز اصلی و برای جلب‌توجه و پذیرش گسترده تلقی می‌شوند.

از ژوئین ۲۰۲۰، کامپاند فایننس[2] با استفاده از رمزارز جدید خود به نام کامپ[3] شروع به اعطای جبرانی به وام‌دهندگان و وام‌گیرندگان روی بستر خود کرد. این رمزارز برای کنترل بستر کامپاند مورد استفاده قرار می‌گیرد اما در بورس‌ها نیز قابل معامله است. پس از آن سایر سیستم‌عامل‌های دیگر از این موضوع پیروی کردند، بدین ترتیب شاهکاری به نام «کشت سود[4]» یا «استخراج نقدینگی[5]» راه‌اندازی شد. کامپ بستری است که در آنجا کاربران، رمزارزهای مختلف را در بین استخرهای گوناگون یک بستر (پلتفرم) و همچنین بین بسترهای مختلف جابه‌جا می کنند تا مجموع سود بیشتری، از جمله سود و کارمزدها را افزایش دهند. اما ارزش توکن‌های اضافه نیز برابر با جوایز گردآوری شده است.

بررسی دای

دای مبتنی بر روش مطمئن ابطال و خرید سهام است که توسط قراردادهای هوشمند میکردائو، در قالب برنامه‌های غیرمتمرکز زنجیره بلوک فعال شده است. کاربرانی که با اتر (یا هر رمزارز دیگر با قابلیت وثیقه‌گذاری) درگیر هستند، قادرند وام به ارزش سپرده اخذ کنند و در نهایت دای جدید را دریافت نمایند. در حال حاضر، نسبت امنیتی اتر روی ۱۵۰٪ تنظیم شده است. این بدان معناست که اگر ۱۵۰ دلار اتر در نظر بگیرید، شما می‌توانید وام تا ۱۰۰ دای (تقریباً صد دلار) دریافت کنید. اگر ارزش وثیقه به زیر این درصد برسد، مبلغ وام اخذ شده معمولاً از طریق قرارداد هوشمند بازپرداخت می‌شود. متقابلاً، در صورت افزایش هزینه، شما می‌توانید دای اضافی قرض بگیرید.

در نتیجه، دای‌های عودت داده شده، پس از بازپرداخت وام و اقساط و بهره افزوده شده،

1. MKR
2. Compound Finance
3. COMP
4. Yield Farming
5. Liquidity Mining

به‌طور خودکار خاموش می‌شود و وثیقه برگشت داده می‌شود. بدین ترتیب، ارزش دلاری دای به واسطهٔ ارزش دلاری وثیقه نزد قراردادهای هوشمند میکردائو پشتیبانی می‌شود.

از طریق تنظیم وثیقه پشتیبان، شرایط وثیقه و نرخ بهره وام یا بهره استیکینگ[1] برای دای میکردائو، می‌تواند میزان دای در گردش را تنظیم کند که به‌طور یکسان بر ارزش کلی آن، تأثیر می گذارد.

دارندگان توکن میکر حق پیشنهاد و اجرای تغییرات در این متغیرها را با استفاده از کد برای خود دارند. دارندگان توکن‌های حاکمیتی می‌توانند در مورد تغییرات پیشنهادی رأی دهند اما درجه متفاوت است و به تعداد بلیط‌های آن‌ها بستگی دارد. توکن میکر به همان اندازه یک ابزار سرمایه‌گذاری در بستر میکردائو است. همراه با مبلغ وام، از بهرهٔ اضافی وام‌دهنده برای خرید و سوزاندن یا در نهایت برداشتن توکن میکر از بازار استفاده می‌شود. این روش برای ایجاد رکود[2] میکر به میزان متناظر با مبلغ وام در نظر گرفته شده است. بیایید در مورد هریک از دسته‌ها علاوه بر میکردائو که ما به آن اشاره کردیم ، یکی‌یکی صحبت کنیم.

کوین ثابت (دارای نوسانات قیمتی بسیار کم)

کوین ثابت یک ارز رمزنگاری‌شده است که برای کاهش نوسانات بیت‌کوین با قیمت ثابت در مقایسه با سبدها یا دارایی‌های «ثابت» طراحی شده است. کوین پایدار می‌تواند به رمزارز پایه، ارز فیات، یا کالاها (برای مثال، فلزات گرانبها یا صنعتی) مرتبط شود. استیبل‌ها یا پایداری‌های قابل حل در ارز، کامودیتی‌ها[3] یا ارز فیات که شناخته شده است قابل پوشش هستند، و کوین‌های پایدار مرتبط با الگوریتم را سینیوریج[4] یا حق‌الضرب می نامند (بدون پشتوانه).

کوین‌های ثابت، ارزهای رمزپایه‌ای هستند که به یک دارایی خارج از جامعهٔ ارزهای رمزپایه مرتبط می‌شوند؛ به‌عنوان مثال دلار یا یورو. هدف اصلی در اینجا ثبات قیمت است.

---

1. Staking Interest Rate

۲. مترجم: وقتی سطح کلی قیمت کاهش می‌یابد تا نرخ تورم منفی شود، به آن رکود گفته می‌شود. همچنین، رکود می‌تواند به سیاست رکودی پولی نظیر بیت‌کوین اشاره کند که دارای موجودی ثابت کوین‌ها است.

3. Commodities
4. Seigniorage

پشتیبان کوین ثابت

مزیت رمزارز پایه مبتنی بر دارایی[1] این است که کوین توسط دارایی‌هایی تثبیت می‌شوند که در خارج از فضای رمزارز پایه در نوسان هستند. از آنجا که بیت‌کوین و آلت‌کوین[2] بسیار با هم ارتباط دارند، دارندگان رمزارزهای پایه نمی‌توانند بدون خروج از بازار یا پناه بردن به یک کوین ثابت مبتنی بر دارایی، از کاهش قابل توجه قیمت جلوگیری کنند. علاوه بر این، اگر این کوین‌ها با حسن نیت اداره شوند و سازوکار بازخرید دارایی داشته باشند، بعید است به دلیل داوری، از ارزش دارایی فیزیکی اساسی کمتر باشد.

تثبیت موازی در معرض نوسان و تغییرپذیری مذکور و ریسک دارایی اساسی قرار دارد. اگر کوین ثابت به روشی غیرمتمرکز محافظت شوند، نسبتاً در برابر شکار (غارت‌گری)[3] محفوظ هستند، اما داشتن بایگانی مرکزی می‌تواند منجر به سرقت یا ضایع شدن اعتماد شود.

کالای مورد حمایت دارایی

ویژگی‌های اصلی پشتیبان‌گیری کوین ثابت:

- یک یا چند مورد ارزش دارد و در صورت لزوم قابل مبادله است (بیشتر یا کمتر).
- شما وعده پرداخت از یک شخص نامنظم و آشفته[4]، یک شرکت باز یا یک مؤسسه مالی تحت نظارت را دارید.
- تعداد کالاهایی که برای نگهداری یک لنگرگاه ثابت[5] استفاده می‌شود، باید منعکس‌کننده موجودی در گردش ثابت باشد.

صاحبان کالاهای مورد حمایت کالاهای ثابت می‌توانند با بازخرید سهام خود با نرخ تبدیل، دارایی واقعی را تصاحب کنند. هزینهٔ حفظ ثبات کوین‌های ثابت، هزینهٔ ذخیره‌سازی و محافظت از مادهٔ اولیه اساسی است. برای مثال، توکن‌های دی.جی. ایکس[6] و سایر موارد را به‌عنوان مثال در نظر بگیرید.

---

1. Asset-based Cryptocurrency
2. Altcoins
3. Predation
4. Unregulated Person
5. Fixed Mooring
6. Digix Gold Tokens

پشتیبان فیات

ارزش این نوع کوین پایدار بر اساس ارزش ارزهای پشتیبانی‌شده در اختیار مؤسسات مالی شخص ثالث تنظیم شده است. اطمینان به در دسترس بودن درمان[1] در این شرایط برای ثبات قیمت بسیار مهم است. درج‌های پشتیبان فیات را می‌توان در بورس اوراق بهادار معامله و از ناشر خریداری کرد. سایر عوامل کلیدی در ثبات کوین‌های ثابت عبارت‌اند از: هزینهٔ حفظ ذخایر و انطباق قانونی، صدور مجوز توسط تنظیم‌کنندگان (رگولاتورها)، نگهداری حسابرسان و زیرساخت‌های کسب‌وکار.

ارزهای رمزنگاری‌شده با ارزهای فیات رایج ترین و اولین نوع کوین‌های ثابت در بازار هستند.

ویژگی‌های رمزارزهای پایه مورد حمایت فیات:

- ارزش آن در یک یا چند ارز (معمولاً دلار آمریکا ، یورو و فرانک سوئیس) با نرخ ثابت، فیکس (ثابت) می‌شود.
- ارتباطات به‌صورت آفلاین از طریق بانک‌ها یا سایر مؤسسات مالی تنظیم‌گری اتفاق می‌افتد که به‌عنوان مخزن ارزهای مورد استفاده برای حمایت از کوین‌های ثابت عمل می‌کنند.
- مقدار ارز مورد استفاده برای حمایت از کوین ثابت باید برابر با کوین ثابت در گردش باشد.

همراه با ارز رمزنگاری‌شده

کوین‌های ثابت مبتنی بر رمزارز پایه، رمزارز پایه را به‌عنوان اوراق بهادار می‌پذیرند و از نظر مفهومی مشابه کوین ثابت مبتنی بر فیات است؛ بااین‌حال یک تفاوت اساسی بین این دو تفسیر این است که درحالی‌که وثیقه فیات به‌طورکلی خارج از زنجیره اتفاق می‌افتد، ارز رمزنگاری‌شده مورد استفاده برای پشتیبانی از این نوع کوین‌های ثابت بلاکچین با استفاده از رویکرد غیرمتمرکز قراردادهای هوشمند ایجاد می‌شود. در بیشتر موارد سود پرداختن بدهی، در موقعی که ارزش ثابت با مسدود کردن وثیقه کاهش می‌یابد، سودآورتر است، تا بدین ترتیب مصرف‌کنندگان بتوانند در معاملات هوشمند وام بگیرند. برای جلوگیری از وقفه‌های ناگهانی، اگر وثیقه خیلی به مبلغ برداشت نزدیک باشد، می‌توانید با یک قرارداد هوشمند وام

1. Treatment

مصرف‌کننده را لغو کنید.

ویژگی‌های اصلی ارز رمزنگاری‌شده بیت‌کوین عبارت‌اند از:

- ارزش ثابت بیت‌کوین توسط سبد دارایی ارز رمزنگاری‌شده یا ارز رمزنگاری‌شدهٔ دیگری ارائه می‌شود.
- الزامی بودن (لازم‌الاجرا بودن) از طریق قراردادهای هوشمند روی زنجیره انجام می‌شود.
- توزیع ثابت بیت‌کوین از طریق قراردادهای هوشمند در داخل زنجیره تنظیم می‌شود.
- با معرفی ابزارها و مشوق‌های اضافی و همچنین وثیقه، به ثبات قیمت دست پیدا کنید.

این نوع اجرای فنی فایل کوین، پیچیده‌تر و متنوع‌تر از خطوط بایگانی مبتنی بر فیات است، در نتیجه خطر بهره‌برداری به دلیل خطاهای کد قرارداد هوشمند (اشکالات) را افزایش می‌دهد، زیرا مودم‌ها به‌صورت زنجیره‌ای کار می‌کنند، لذا آن‌ها مشمول مقررات شخص ثالث نیستند که راه‌حل‌های غیرمتمرکز ایجاد کنند. جنبهٔ بالقوه مشکل‌ساز این نوع کوین‌های ثابت، برابر با تغییر در ارزش اوراق بهادار زیر بنایی و بسترهای (پلتفرم‌های) هاستینگ[1] است. پیچیدگی و پشتیبانی غیرمستقیم کوین‌های ثابت می‌تواند کاربرد آن‌ها را محدود کند؛ زیرا درک نحوه ارائه قیمت دشوار است. با توجه به ماهیت بسیار ناپایدار و بسیار همگرا در بازار ارزهای رمزنگاری‌شده، وثیقهٔ بسیار بزرگ نیز باید حفظ شود تا ثبات حاصل شود.

تبادل غیرمتمرکز

دی.ای.ایکس[2] (ارز غیرمتمرکز) یکی از انواع مبادلات ارز رمزنگاری‌شده است که معاملات مستقیم همتا به همتا با رمزارزهای پایه را به‌صورت آنلاین، ایمن و بدون واسطه امکان پذیر می‌کند.

در معاملات انجام شده از طریق مبادلات غیرمتمرکز، بلاکچین معمولاً با سازمان‌های شخص ثالث معمولی جایگزین می‌شود که بر اوراق بهادار دفاتر کل عمومی و غیرمتمرکز و انتقالات دارایی نظارت دارد (برای مثال بانک‌ها، کارگزاران اوراق بهادار، درگاه‌های پرداخت آنلاین، مقامات و غیره). روش‌های معمول کار، شامل استفاده از قراردادهای هوشمند یا ارسال مجدد سفارشات است؛ اما گزینه‌های بسیار دیگری و همچنین تنوع درجات مختلف تمرکززدایی نیز امکان دارد.

1. Hosting Platforms.
2. DEX (Decentralized Exchange)

با کمک مبادلات آنلاین، کاربران می‌توانند ارزهای خود را با ارزهای دیگر مبادله کنند؛ چه با بیت‌کوین و چه با دلار آمریکا یا دای. دی.ای.ایکس نیز مبادلات درجه یک و داغی است که کاربران را مستقیماً به‌هم متصل می‌کند تا تجارت امیدوارکنندهٔ ارزهای رمزپایه را، بدون وابستگی به واسطه تضمین کنند و بدین ترتیب آن‌ها روی پول خود کار کنند.

صرافی‌های غیرمتمرکز خطر سرقت از صرافی‌های هک شده را کاهش می‌دهد، زیرا مصرف‌کنندگان نیازی به انتقال دارایی‌های خود به صرافی مذکور را ندارند. مبادلات پیشرفته همچنین می‌توانند از دست‌کاری قیمت یا حجم معاملات تقلبی از طریق فلاشینگ جلوگیری کنند و بیشتر از موضوع «شناسایی مشتری فعال» ناشناخته هستند. مبادلات مشتری[1] خود را بشناسید.

نشانه‌هایی وجود دارد که مبادلات غیرمتمرکز از حجم معاملات کم و نقدینگی بازار رنج می‌برند. پروژه 0x، که پروتکلی برای ایجاد مبادلات غیرمتمرکز با نقدینگی نامطلوب است، در تلاش برای حل این مشکل است.

معایب

از جایی که هیچ فرآیند «شناخت مشتری» وجود ندارد و معامله غیرقابل‌برگشت است، در صورت هک شدن کاربران و دریافت رمزهای عبور یا کلیدهای خصوصی آن‌ها، شما کاربران را از دست خواهید داد. اگرچه صندوق نقدینگی دی.ای.ایکس بیشترین استفاده را دارد اما ممکن است اشکالاتی نیز داشته باشد. رایج‌ترین مشکلات صندوق‌های نقدینگی دی.ای.ایکس کاهش قیمت و افزایش عملکرد است.

کاهش قیمت‌ها به دلیل ماهیت سازندگان بازار خودکار[2] است. هرچه معامله بزرگتر باشد، بیشتر بر قیمت تأثیر می‌گذارد. برای مثال، اگر از یک محصول ثابت سازندگان بازار خودکار استفاده می‌کنید، همهٔ معاملات باید محصول $XY = k$ را ثابت نگه دارند در جایی که x و y تعداد دو رمزارز پایه (یا توکن) موجود در مجموعه هستند. هرچه اندازه ورودی Δx بزرگتر باشد، نسبت نهایی y / x پایین تر است و قیمت مبادله را می‌دهد. این مسئله معمولاً برای شرکت‌های بزرگ یا استخرهای کوچک نقدینگی مهم است.

راه‌اندازی فرونتال (شدید و مستقیم) فرم خاصی از حمله بلوک عمومی است که در آن شرکت‌کنندگان (معمولاً کارگران معدن) با دیدن معامله قریب‌الوقوع، معاملات خود را انجام می‌دهند (به‌عنوان مثال، با هزینه‌های معامله بازی می‌کنند) و سود معاملهٔ اولیه را کاهش می‌دهد.

---

1. KYC
2. Automated Market Makers (AMM)

ایده‌ها برای بهبود مقاومت در برابر کشش محصولات دائمی بازارساز خودکار، برای اولین‌بار در یک پست توسط ویتالیک بوترین[1] مورد بحث قرار گرفت. یک راه‌حل ممکن این است که معامله‌هایی را در نظر بگیریم که بلافاصله انجام نمی‌شوند اما مدتی ادامه دارند (به‌عنوان مثال ۵ دقیقه). در این صورت نقدینگی به تدریج و بدون بالاترین قیمت به استخر منتقل می‌شود. این مسئله ادامه سفر را برطرف می‌کند، زیرا کارگران خط مقدم نمی‌توانند از کار طولانی بهره‌مند شوند؛ همچنین به جلوگیری از لغزش قیمت کمک می‌کند، زیرا واسطه‌ها و دیگر بازرگانان می‌توانند به‌طور موازی عمل کنند و مانع معامله‌گران طرف مقابل شوند.

درجات تمرکززدایی

صرافی‌های غیرمتمرکز هنوز هم ممکن است دارای یک مؤلفه مرکزی باشند؛ بدان معنا که برخی کنترل‌ها در خصوص صرافی در دستان مؤسسات مرکزی باقی خواهد ماند. یک مثال خوب این است که آیدیکس[2] مانع از ثبت سفارش کاربران ایالت نیویورک در سیستم عامل می شود.

در ژولای ۲۰۱۸، گزارش شده بود که بورس اوراق بهادار غیرمتمرکز بانکور[3] هک شد و باعث خسارت دارایی ۱۳,۵ میلیون دلار قبل از مسدود شدن بودجه شد. اپراتورهای مبادلات پیشرفته می‌توانند پیامدهای قانونی را از مقامات نظارتی ایالتی به‌دست آورند. به‌عنوان مثال بنیانگذار ایثردلتا[4]، که در نوامبر ۲۰۱۸ هزینه‌ای را به ایالات متحده پرداخت کرد. کمیسیون بورس و اوراق بهادار یک بورس سهام خصوصی را اداره می کند.

کامپاند

در این دسته، تعداد کمی محصولات متفاوت و مهم «امور مالی غیرمتمرکز» وجود دارند. کامپاند یکی از مهمترین آنهاست. در زمان نگارش این متن کامپاند بزرگترین پروژه در دسته‌بندی وام‌دهی[5] با حدود ۶۳۰ میلیون دلار ارزش دارایی مسدود شده در این پروتکل است. کامپاند یک پروتکل نرخ سود (بهره) الگوریتمیک است که به کاربران، اجازهٔ تولید و عرضهٔ دارایی‌ها مثل

1. Vitalik Buterin
2. IDEX
3. Bancor
4. EtherDelta
5. Lending

اتریوم یا تِتِر[1] را داده و شروع به ایجاد سود می‌کند. دارایی‌های عرضه شده می‌توانند مالکانشان را قادر به جذب و دریافت دارایی‌های دیگر نمایند.

سیاست‌های دادوستد (وام‌دهی و استقراض) بدون واسطه[2] از مهمترین کاربردها در محیط و اکوسیستم امور مالی غیرمتمرکز هستند. برای مثال کامپاند از یک الگوریتم با پروتکل نرخ سود مستقل استفاده می‌کند که با فهرست بلندی از بسترهای امور مالی غیرمتمرکز مانند پوول توگدر[3]، دی.هارما[4] و آرجنت[5] ترکیب شده و زیربنای آن‌ها را نیز تشکیل می‌دهد.

با فراهم کردن بازارهای نرخ سود در اتریوم، کامپاند به کاربران امکان بدست آوردن سود در ارزهای رمزنگاری شده را می‌دهد که با استخر وام دهی تامین شده است. قراردادهای هوشمند کامپاند به طور اتوماتیکوار داد وستدکنندگان را با یکدیگر متناسبسازی می‌کند. سپس به منظور پشتیبانی از سرمایه‌گذاری، نرخ سود را بر اساس درصد دارایی‌های وام گرفته شده محاسبه می‌کند. کامپاند یک مثال واضح از موقعیت نمایی در دامنهٔ امور مالی غیرمتمرکز است. با ادغام محصولات بیشتری در سیاست‌های کامپاند، سرمایه‌گذاری‌ها در حوزهٔ رمز ارز، سود بیشتری بدست خواهند داد، حتی زمانی که غیرفعال باشند.

کامپاند وام‌هایی را برای برخی رمزارزها مانند هوزینگ (دای)[6]، ایثر (ای.تی.اچ)[7]، کوین یو.اس.دی (یو.اس.دی.سی)[8]، اوکس (زد.آر.ایکس)[9]، تتر (یو.اس.دی.تی)[10]، رپت.بی.تی.سی (دبلیو.بی.تی.سی)[11] و توکن دارای نقش اساسی[12]، رمزارز آگور[13] و سای[14] فراهم می‌آورد. هر صاحب یا دارندهٔ رمزارز می‌تواند به‌طور مستقیم رمزارز را قرض بگیرد یا قرض بدهد. بدون اینکه اتلاف وقت، زحمت یا صرف هزینهٔ ارتباط با واسطه‌های مالی سنتی داشته باشد.

اگر شما مالک رمزارزهای یاد شده در متن بالا باشید، می‌توانید آن را ارسال، بلوکه،

---

1. Tether
2. User to User
3. PoolTogether
4. Dharma
5. Argent
6. Housing (DAI)
7. Ether(ETH)
8. USD Coin (USDC)
9. Ox (ZRX)
10. Tether (USDT)
11. Wrapped BTC (WBTC)
12. Basic Featured Token (ATM)
13. Augur (REP)
14. Sai (SAI)

سپرده‌گذاری یا قرض کنید. تمام این‌ها از مزایای پروتکل کامپاند است. قفل کردن رمزارز با کامپاند، مشابه سپردن پول در یک حساب پس‌انداز است با این تفاوت که از یک پروتکل غیرمتمرکزشده بر اساس بلاکچین استفاده می‌کند. به‌جای سپرده‌گذاری پول در بانک، رمزارزها به کیف پول ارسال می‌شود. شما بلافاصله شروع به کسب سود در رمز ارز می‌نمایید، درست همانند سپرده‌گذاری در یک بانک. نرخ بازده با همان نمادی نشان داده می‌شود که قرض گرفته شده است. به بیان دیگر، ارسال نماد بی.آ.تی[1]، به‌صورت نماد بی.آ.تی سود کسب می‌کند و ارسال نماد دای، به‌صورت نماد دای سود به دست میآورد. رمزارزی که شما ارسال می‌کنید، در صندوق بسیار عظیمی از نمادهای مشابه جمع می‌شود که از هزاران نقطهٔ دنیا ارسال شده است.

وجه دیگر این معادله وام است. بلوکه کردن رمزارز در کامپاند به شما اجازه دریافت وام می‌دهد. بعضی بسترها نیازی به چک‌های اعتباری ندارند؛ بنابراین هر شخص در هر کجای دنیا با استفاده از رمزارز می‌تواند برای درخواست وام اقدام نموده و بلافاصله در صورت احراز شرایط لازم، درخواست او تصویب می‌شود.

کامپاند کیفیتی از دارایی است که می‌تواند مقدار وام شما را تعیین کند. به‌طور مثال اگر شما بیت‌کوین به ارزش ۵۰۰ دلار را به هزار کامپس[2] تبدیل کنید، کامپاند سقف وام بیت‌کوین را تا ۵۰ درصد تعیین می‌کند (که به عنوان یک فاکتور امنیتی نیز شناخته می‌شود)، شما می‌توانید ۲۵۰ دلار برای رمز ارزهای دیگری که بوسیله پروتکل کامپاند پشتیبانی می‌شود را قرض دهید. (لیست بالا را ببینید). درست مانند زمانی که پولی را از بانک قرض می‌کنید، شما لازم است سود آن را پرداخت کنید.

پس اینجا سپرده‌ها و وام‌هایی وجود دارند که لازم است برای هر دو نرخ سود در نظر گرفته شود. شما بر اساس مبلغ وام دریافتی، سودی را پرداخت می‌کنید. اجازه بدهید درباره این صحبت کنیم که چگونه با استفاده از یک سیستم خوش‌ساخت که به زیبایی معماری شده است، به‌طور اتوماتیک‌وار این نرخ‌ها محاسبه و اعمال می‌شوند.

خواه در حال وام گرفتن باشید و خواه در حال تجارت و کسب‌وکار، ابتدا لازم است رمز ارز را توسط کامپاند تبدیل کنید. در این حالت شما توکن یا توکن‌های مختلطی[3] دریافت خواهید کرد که در عوض نشان‌دهندهٔ توازن رمزارز شما با مقدار دریافتی است. این توکن و بسیاری

1. BAT
2. COMPS
3. cToken

توکن‌های دیگر به‌عنوان یک ای.آر.سی [1] ۲۰در بلاکچین اتریوم تولید می‌شوند. توکن‌های ای.آر.سی ۲۰ یکی از بزرگ‌ترین مزیتها و نوآوری‌های بازار رمز ارز بر پایهٔ بلاکچین هستند. سود عایدی (یا پرداخت شده) می‌تواند انتقال داده شود، فروخته شود یا برای دیگر برنامه‌های غیرمتمرکز [2] در زیستبوم امور مالی غیرمتمرکز برنامه‌ریزی شود (درست مانند هر توکن اتریوم دیگری). با این توکن‌ها به‌گونه‌ای رفتار کنید که دارایی‌های دیجیتال در بلاکچین اتریوم با رمزهای عمومی یا خصوصی مدیریت می‌شدند.

نرخ‌های سود به میزان رمزارز (یا نقدینگی) موجود در هر بازار و در زمان واقعی به عرضه و تقاضا بستگی دارد تا شرایط فعلی بازار را منعکس کند. نرخ‌های سود نمایش داده شده, به‌عنوان نرخ‌های سود سالانه ردیف می‌شوند و هر زمان که یک بلاک اتریوم شکسته شود، شروع به کار می‌کنند. در هر ۱۵ ثانیه، مقدار توکن‌ها با ضریب ۱/۱۲۱۰۲۴۰۰(بلاک‌های ۱۵ ثانیه‌ای در سال) از درصد سالانهٔ اعلام شده توسط رمزنگار کریپتوپدیا [3] در آن زمان افزایش می‌یابند.

یک پروژهٔ محبوب دیگر امور مالی غیرمتمرکز، آوه [4] است که از قراردادهای هوشمند و نیز مشوقه‌ای خرمندانهٔ خاص استفاده می‌کند. در اینجا ما می‌توانیم ارز دیجیتال باثبات یا استیبل کوین تولید کنیم که به دلار آمریکا مرتبط می‌شود، بدون اینکه مجبور به ذخیرهٔ دلار در دنیای واقعی باشیم. تعداد زیادی ارزهای دیجیتال موهومی [5] (مجازی) غیرالگوریتمی دیگر وجود دارند؛ مانند یو.اس.دی.تی [6]، یو.اس.دی.سی [7] و یا پی.آ.سی [8]. بزرگترین مشکل آنها متمرکز بودنشان است، زیرا این نوع ارزهای دیجیتالی به‌وسیلهٔ یک شرکت پشتیبانی می‌شوند که مسئولیت ذخیرهٔ دارایی زیربنایی متناظر با آنها را دارد و می‌تواند دلار آمریکا یا هر دارایی دیگر باشد.

به‌هرحال ارزهای دیجیتالی باثبات محبوبیت زیادی به دست آورده‌اند و اغلب به‌عنوان یک کامپاند یا نوع دیگری از پروژه‌ها در اپلیکیشن امور مالی غیرمتمرکز، استفاده می‌شوند. متفاوت با رمزارزهای مرکزی، صرافی‌های غیرمتمرکز یا دیکس، به رمزارزها اجازهٔ مبادله با یک روش کاملاً غیرمتمرکز و غیرمجاز و همچنین بدون جلوگیری از ذخیرهٔ سکه را می‌دهد. مثالی از

1. ERC-20
2. Dapps
3. n.d
4. AAVE
5. Dummy
6. USDT
7. USDC
8. PAC

مبادلات غیرمتمرکز در استخرهای نقدینگی، یونی سواپ[1]، کایبر[2]، بالانسر[3] و بانکور هستند. لینکس[4] و آیدکس[5] نیز نمونه‌هایی از سامانه‌های سفارش کتاب هستند.

اوراق مشتقه[6]

مشابه با امور مالی سنتی، اوراق مشتقه، قراردادهایی هستند که ارزش آنها با توجه به بازده دارایی اساسی تعیین می‌شود. برنامهٔ اصلی امور مالی غیرمتمرکز در این فضا، *مصنوعی‌ها*[7] هستند که یک بستر غیرمتمرکز شده است، و دارایی‌های گوناگونی را روی زنجیره فراهم می‌کنند. اوراق مشتقه محصولاتی هستند که ارزششان توسط یک متغییر یا بیشتر که پایه[8] (دارایی‌های اساسی) نامیده می‌شوند، تعیین می‌شود. این پایه می‌تواند یک دارایی، یک شاخص یا یک نرخ سود و اغلب فقط به عنوان «خط مبنا[9]» شناخته شود. اوراق مشتقه می‌توانند برای اهداف گوناگونی شامل «بیمه (پوشش ریسک) در مقابل حرکت قیمت، در معرض حرکت قیمت با حدس و گمان قرار گرفتن، و یا دسترسی به داراییها یا بازارهای سخت معامله» به کار روند.

قردادهای هوشمند مبتنی بر اتریوم، در ایجاد اوراق مشتقهٔ توکن‌سازی‌شده کمک می‌کنند به طوری که ارزش آنها از یک موفقیت در سرمایه‌گذاری زیربنایی به دست می‌آید که از طریق آن توافقنامه‌های شرکا به‌صورت کدشده، بسته شده است. همچنین اوراق مشتقهٔ امور مالی غیرمتمرکز، می‌توانند سرمایه‌گذاری در دنیای واقعی را نشان دهند؛ مانند ارزهای تخت[10]، اوراق قرضه، کالاها و حتی رمز ارزها.

متداولترین اوراق مشتقهٔ مالی شامل آتیها، اختیارها، مبادله‌ای‌ها و تبدیل‌هایی مانند وثیقه‌های مصنوعی [11]و سوآپ‌های اعتباری[12] هستند. بیشترین اوراق مشتقه در صرافی‌های

1. Uniswep
2. Khyber
3. Balancer,
4. Links
5. Idex
6. Derivatives
7. Synthetixes
8. base
9. baseline
10. flat currencies
11. synthetic collateral
12. credit swaps

فرابورس[1] یا صرافیهایی مانند شیکاگو مرکانتیل[2] مبادله می‌شوند، درحالیکه قراردادهای بیمه به‌عنوان صنعت جداگانه‌ای توسعه می‌یابند.

اوراق مشتقه در لیست اجزای اصلی ابزارهای مالی در مکان نخست قرار دارند و دو تای بعدی سهام و بدهی‌ها هستند (مانند اوراق قرضه و وثیقه رهن‌ها). اوراق مشتقه به‌عنوان توافقات قراردادی بین دو یا چند طرف هستند که شرایط پرداخت بین طرفین (به‌ویژه تاریخ، مقدار و تعریف متغیرهای اساسی، تعهدات قراردادی طرفین و مبالغ ساختگی و غیرواقعی[3] را تعریف می‌کنند.

دارایی‌هایی شامل سهام، کالاها، اوراق قرضه، نرخ‌های سود و ارزها می‌توانند اوراق مشتقهٔ دیگری باشند که لایهٔ دیگری را ایجاد کرده و ارزیابی دقیق را پیچیده می‌کنند.

معامله مارجینگ[4]

درحالی‌که معامله‌گران مارجینگ می‌توانند با وام گرفتن از کارگزار (دلال)– که وثیقه وام را تشکیل می‌دهد – بر معاملاتشان در امور مالی متعارف تأثیر بگذارند، از طرف دیگر، معامله مارجینگ در امور مالی غیرمتمرکز، با استفاده از سیاست‌های وام غیرمتمرکز و غیرمتصدیانه (غیرحضانتی)[5] مانند کامپاند، فالکروم[6] و دی.وای.دی.ایکس[7] انجام می‌شود. به دلیل مکانیزاسیون قراردادهای هوشمند کارگزاریهای متعارف، برخی به سمت بازارهای پولی مستقل در بستر امور مالی غیرمتمرکز سوق پیدا کرده‌اند.

بیمه[8]

بیمه بخش دیگری از امور مالی سنتی است که می‌تواند در امور مالی غیرمتمرکز بازتولید شود. همچنین بیمه، ضمانت پرداخت جبران خسارت بابت پرداخت حق بیمه را فراهم می‌کند. یکی از پرکاربردترین برنامه‌های بیمه در فضای امور مالی غیرمتمرکز مربوط به موارد خطای قرارداد هوشمند و محافظت از سپرده است. معروفترین پروژه‌های امور مالی غیرمتمرکز در این زمینه

1. OTC
2. Chicago Mercantile
3. Fictitious Amounts
4. Margin Trading
5. Non-custodial
6. Fulcrum
7. DYdX
8. Insurance

نکسوس[1]، میوچوآل[2] و اوپین[3] هستند.

امور مالی غیرمتمرکز هنوز یک دامنهٔ آتی و قریب‌الوقوع است و خطرات مربوط به خطاهای قرارداد هوشمند و نقض‌ها و تخلفات پیرامون آن‌ها را دارد. برخی از گزینه‌های بیمهٔ خلاقانه برای کمک به کاربران در پوشش خرید، برای محافظت از دارایی‌هایشان به بازار آمده‌اند. نکسوس میوچوآل[4] یکی از راه‌حل‌های ارائه شده است. این یک پوشش قرارداد هوشمند ایجاد می‌کند که از استفادهٔ غیرعمد از کد قرارداد هوشمند محافظت می‌کند.

بخش مالی بسیار مهم اما نه‌چندان محدود در اکوسیستم امور مالی غیرمتمرکز، خدمات اُوراکِل[5] است که متمرکز بر ارائه جریان داده‌های پایدار خارج از قراردادهای هوشمند است. مشهورترین پروژه در این زمینه «چین لینک[6]» است. این‌ها تقریباً در تمام بخش‌های اصلی بستر امور مالی غیرمتمرکز یافت می‌شوند. همچنین میتوان آن را به روش‌های مختلف ترکیب کرد.

شما می‌توانید آن را به‌عنوان لِگو پول[7] تصور کنید، زیرا می‌توانید محصولات پیچیده‌تری از امور مالی غیرمتمرکز را در بالای بلاک های موجود بسازید.

هویت[8]

با همکاری سیستم‌های هویت مبتنی بر بلاکچین، پروتکل‌های مالی غیرمتمرکز راهی برای کمک به کاربران قفل شده است که قبلاً به یک سیستم اقتصادی واقعی جهانی دسترسی پیدا کرده‌اند. راه‌حل‌های امور مالی غیرمتمرکز، با به حداقل رساندن وثیقهٔ مورد نیاز برای افرادی که بودجه اضافی ندارند، به آن‌ها کمک می‌کند و از طریق ویژگی‌های مربوط به شهرت و فعالیت مالی به‌جای استفاده از داده‌های رایج، مانند درآمد و مالکیت، به اعتبار کاربران یاری می‌رساند.

دنیای امور مالی غیرمتمرکز، رازداری داده‌های مربوط به اطلاعات هویتی شخصی و همچنین دسترسی آزاد را تشویق می‌کند؛ بنابراین هرکسی که به اینترنت متصل باشد، آزاد است که با حفظ کنترل داده‌ها و سرمایه‌گذاری‌های خود به برنامه‌های امور مالی غیرمتمرکز دسترسی پیدا کند.

---

1. Nexus
2. Mutual
3. Opyn
4. Nexus Mutual
5. Oracle
6. Chain Link
7. Lego Money
8. Identity

بازی کردن[1]

قابلیت ترکیب‌پذیری امور مالی غیرمتمرکز فرصت‌هایی برای توسعه‌دهندگان محصولات ایجاد کرده است، که سیاست‌های امور مالی غیرمتمرکز را به‌طور مستقیم، از طریق ترکیب ستونی، در بسترها ایجاد کنند. بازی‌های مبتنی بر اتریوم به دلیل اقتصادهای داخلی و استانداردهای تشویقی خلاقانه، به یک مورد مشهور در استفاده از امور مالی غیرمتمرکز تبدیل شده‌اند. برای مثال «پول توگدِر» یک قرعه‌کشی پس‌انداز بدون ضرر است که کاربران را قادر می‌سازد با واریز استیبل کوین دای، بلیط‌های دیجیتال را خریداری کنند؛ طوری که سپس ترکیب شده و به سود پروتکل بازار پول کامپاند وام می‌دهد.

یکی از اصول اصلی طراحی سیاست‌های امور مالی غیرمتمرکز، سازگاری است که به این واقعیت اشاره دارد که اجزای مختلف سیستم می‌توانند به‌راحتی به یکدیگر متصل شده و از یکدیگر استفاده کنند. از طیف گسترده‌ای از برنامه‌های کاربردی یکپارچه امور مالی غیرمتمرکز، می‌توان دریافت که کد قابل ساختن، تأثیر شبکه‌ای قدرتمند در جامعه ایجاد کرده است؛ به‌گونه‌ای که همچنان بر اساس چیزهایی ساخته می‌شود که دیگران ایجاد کرده‌اند. بسیاری روند توسعه امور مالی غیرمتمرکز را با ساخت لِگوها مقایسه می‌کنند و به همین سبب با نام مستعار معروف «مانی لِگو» شناخته می‌شوند.

توسعه‌دهندگان اتریوم و تیم‌های تولیدی اکنون می‌توانند سیاست‌های امور مالی غیرمتمرکز را با بستهٔ ابزاری کامل و ادغام‌های امنیتی مورد نیاز، به‌ویژه از آزادی‌های قرارداد هوشمند ترافل[2]، مجموعه آ.پی.آی اینفورا[3] و ابزارهای بهادار بایسته[4] ایجاد و آغاز کنند.

تجزیه و تحلیل داده‌ها[5]

با توجه به شفافیت خارق‌العاده آن‌ها در مورد داده‌های تراکنش و فعالیت شبکه، سیاست‌های امور مالی غیرمتمرکز مزایای مشخصی برای کشف داده‌ها، تجزیه و تحلیل و تصمیم‌گیری در مورد فرصت‌های مالی و کنترل ریسک می‌دهد. رشد نامنظم و متغیر برنامه‌های جدید مالی غیرمتمرکز باعث تحریک ابزارها و داشبوردهای مختلفی، مانند داده‌های دیفای پالس[6] و

1. Gaming
2. Truffle
3. API Infura
4. Diligence›s security tools
5. Data and analytics
6. DeFi Pulse

کودیفای[1] شده است. این به کاربران کمک می‌کند تا مقدار قفل شده در سیاست‌های امور مالی غیرمتمرکز را ردیابی کنند، ریسک سیستم‌عامل را بررسی کرده و مفاهیم عملکرد (کشت) و نقدینگی را از یکدیگر تفکیک کنند. داده‌های کودیفای، وظیفهٔ تشخیص عملکرد از نقدینگی و سایر عوامل را در سیاست‌های امور مالی غیرمتمرکز دارد.

دائوها

سازمان خودمختار غیرمتمرکز یا دائو با توجه به مقررات شفاف رمزگذاری‌شده در بلاکچین اتریوم همکاری می‌کند. در نتیجه تمایلات برای یک بخش سازمانی و متمرکز را از بین می‌برد. سایر پروتکل‌های معروف در نظام مالی غیرمتمرکز مانند میکر[2] و کامپاند[2]، در دائوها، آغازگر افزایش سرمایه، مدیریت عملیات مالی و تمرکززدایی مدیریت برای مردم بوده‌اند.

سازگاری یا انطباق[3] و شناسایی تراکنش شما [4]

در امور مالی معمول (مرسوم) پیروی از مبارزه با پول‌شویی[5] و مقابله با تأمین مالی تروریسم[6] بستگی به راهنمای «مشتری خود را بشناس»[7]، دارد. در خلأ نظام مالی غیرمتمرکز، زیرساخت‌های غیر متمرکز اتریوم به تحلیل اطاعت‌پذیری نسل بعدی پیرامون رفتار آدرس‌های کمکی به‌جای فردگرایی شرکت‌کننده کمک می‌کند. این ابزار «تراکنشت را بشناس» ما را قادر ساخته تا ریسک را در زمان کافی ارزیابی نموده و در مقابل کلاهبرداری و سایر جرایم مالی دفاع کنیم.

مدیریت دارایی

کیف پول‌های رمزنگاری‌شده مانند متا ماسک[8]، آرجنت[9] و جی نویسس ایمن[10] شما را قادر می‌سازد تا بدون دردسر و با اطمینان با برنامه‌های غیر متمرکز برای انجام هر کاری از قبیل خرید، فروش و انتقال رمزارز گرفته تا دریافت سودتان از سرمایه‌گذاری دیجیتال ارتباط برقرار

1. CoDeFi
2. Maker
2. Compund
3. Know-your-transaction
4. KYT
5. AML
6. CFT
7. Know-your-customer
8. MetaMask
9. Argent
10. Gnosis Safe

کنید. شما حافظ سرمایهٔ رمزارز خودتان با نظام مالی غیرمتمرکز هستید.

این بدان معنی است که شما خودتان صاحب اطلاعات‌تان در فضای نظام مالی غیرمتمرکز هستید و آن را تماماً توسط خودتان کنترل می‌کنید. برای مثال متاماسک عبارت بازیابی[1]، رمزهای عبور و کلیدهای شخصی شما را در یک طرح رمزنگاری‌شده روی دستگاه شما طبقه‌بندی می‌کند تا فقط شما بتوانید به حساب‌ها و اطلاعات خودتان دسترسی داشته باشید.

مکان‌های بازار[2]

سیاست‌های نظام مالی غیرمتمرکز، افزایش قابل توجهی در مجموعه بازارهای آنلاین داشته است و به کاربران اجازه می‌دهد محصولات و خدمات را در سطح بین‌المللی از یک کاربر به کاربر دیگر مبادله کنند. این موارد از کدهای برنامه نویسی مستقل، مجموعه‌های دیجیتال، یا توکن‌های غیرقابل تعویض[3] گرفته تا جواهرات و پوشاک واقعی را شامل می‌شود.

پرداخت‌ها

پرداخت کاربر به کاربر بدون شک، دلیل اصلی استفاده از دامنهٔ نظام مالی غیرمتمرکز و اکوسیستم بلاکچین به‌طورکلی است. فناوری بلاکچین تمام متصل است تا کاربران بتوانند با خیال راحت و مستقیم ارز رمزنگاری‌شده را بدون حضور واسطه‌ها معامله کنند. راه‌حل‌های پرداخت نظام مالی غیرمتمرکز، یک سیستم اقتصادی آزادتر ایجاد می‌کند برای مردمی که دسترسی به بانک ندارند و بدون بانک هستند و به مؤسسات مالی بزرگ کمک می‌کند تا زیرساخت‌های بازار را ساده و کارآمد کنند و به مشتریان عمده و خرده‌فروش بهتر خدمت کنند.

بازارهای پیش‌بینی[4]

بازارهای پیش‌بینی مبتنی بر بلاکچین مانع استدلال و تعقل مردم می‌شوند و به کاربران کمک می‌کنند تا در نتیجهٔ رویدادها، رأی دهند و ارزش مبادله‌ای را به اشتراک بگذارند. سپس قیمت‌های بازار تبدیل به نشانگرهای زیادی برای احتمال وقوع یک رویداد می‌شوند. یک مثال از یک پلتفرم محبوب نظام مالی غیرمتمرکز برای شرط بندی، آرگور[5] است؛ این برنامه، بازارهای پیش‌بینی را بر اساس نتایج رأی‌گیری، رویدادهای اقتصادی و بازی‌های ورزشی دارای اهمیت می‌سازد.

---

1. Seed phrase نوع رمز ریشه‌ای و پایه‌ای است که با داشتن آن می‌توان به سایر رمزها دسترسی پیدا کرد
2. Market Places
3. Non-fungible tokens نوعی توکن غیر قابل تبدیل به واحدهای کوچک‌تر
4. Prediction markets
5. Argur

پس‌انداز

بسیاری از برنامه‌های نظام مالی غیرمتمرکز مانند کامپاند[1] حساب‌های بهره‌ای و سودده ارائه می‌دهند که بر اساس سیاست‌های استخر وام‌دهی است و می‌تواند به‌صورت نمایی بیش از نوع حساب‌های پس‌انداز معمولی باشد که بر اساس نرخ بهرهٔ پویا و مرتبط با عرضه و تقاضا است. برخی از برنامه‌های پس‌انداز محبوب آرجنت، دی. هارما و پول توگدر هستند که مورد آخر، یک بازی پس‌انداز بدون ضرر است که در آن بازیکنان حتی در صورت پیروزی یا عدم پیروزی تمام پول خود را پس می‌گیرند.

فعالیتی که در اطراف این ابزارهای پس‌انداز خلاقانه پدیدار شده، «کشت سود[2]» است. کشت سود به کاربرانی اشاره دارد که برای افزایش بازده، سرمایه‌گذاری رمزارز غیرفعال خود را در پروتکل‌های مختلف نقدینگی جابه‌جا می‌کنند. شور و هیجان پیرامون (برنامه) کشت سود در نظام مالی غیرمتمرکز باعث ایجاد انگیزه شده است و «ایده‌های میمی» را در اینترنت موجب شده است.

شرط‌بندی[3]

با تغییر شبکه اتریوم به الگوریتم توافق گواه اثبات سهام[4] با فاز ۰ از اتریوم ۲,۰ ، کاربران اکنون این فرصت را دارند که اتر[5] خود را در نظر بگیرند و چه به‌عنوان اعتبارسنج و چه از طریق ارائه‌دهندگان سهام، پاداش دریافت کنند. شرط‌بندی سهام در اتر ۲ [6] مشابه حساب پس‌انداز بهره‌دار است که در آن سهام، به‌خاطر ارزیابی بلاک‌ها قبل از اضافه شدن به بلاکچین، سود و بهره به آن‌ها تعلق می گیرد.

توکن‌سازی[7]

این موضوع، یکی از مبانی امور مالی غیرمتمرکز و عملکرد بومی بلاکچین اتریوم است. توکن‌ها نه تنها شبکه را تأمین می‌کنند بلکه تنوع امکانات اقتصادی را نیز باز می‌کنند. به زبان

1. Compound
2. Yield farming
3. staking
4. Proof of Stake
5. ETH
6. Eth2
7. Tokenization

ساده، توکن یک دارایی دیجیتالی است که در بلاکچین توسعه، اعطا و هدایت می‌شود. توکن‌ها به‌گونه‌ای ساخته می‌شوند که ایمن و بلافاصله قابل جابه‌جایی باشند و با یک سری قابلیت‌های داخلی برنامه‌ریزی شده‌اند.

توکن‌های مبتنی بر اتریوم از توکن‌های بهادار املاک و مستغلات که خصوصیات تکه‌تکه‌شده را نشان می‌دهند تا توکن‌هایی با پلفترم خاص که با انگیزه استفادهٔ یک برنامه خاص، به‌عنوان گزینه‌ای امن و دیجیتالی برای دسترسی، مبادله و ذخیره ارزش برای کاربران در سرتاسر جهان افزایش یافته است.

معامله‌گری[1]

در فضای نظام مالی غیرمتمرکز، معاملات شامل طیف وسیعی از معاملات مشتقات، معاملات مارجین[2] (اعتباری) و مبادله‌های توکن است. این امر در سراسر شبکهٔ رو به رشد و ادغام شده از معاملات، گروه‌های نقدینگی[3] و بازار اتفاق می‌افتد. معامله‌گران رمزنگارش در مبادلات غیرمتمرکز از هزینه‌های کمتر ارز، تسویه‌حساب سریع و مالکیت کامل دارایی‌های خود سود می‌برند.

امور مالی غیرمتمرکز (نظام مالی غیرمتمرکز) در مقابل امور مالی متمرکز[4]

بیایید تفاوت کلیدی بین نظام مالی غیرمتمرکز و امور مالی متمرکز، به‌معنای اقتصاد مرکزی یا سنتی را مقایسه کنیم؛ اما اگر قبلاً این کار را انجام داده‌اید، دکمه اشتراک‌گذاری را فشار دهید تا این کانال رشد کند.

امور مالی متمرکز	نظام مالی غیرمتمرکز
سیستمی بر پایه مجوز	بدون نیاز به مجوز
نیازمند به شناخت مشتری خود	نیازی به پروتکل شناخت مشتری شما نیست
منبع بسته – تصمیمات پشت درهای بسته	منبع باز – تشویق به همکاری رایگان
امور مالی متمرکز روی پایه‌های قدیمی تولید می‌شود.	نظام مالی غیرمتمرکز روی بلاکچین تولید می‌شود.

1. Trading
2. Margin Trading
3. Liquidity pool گروه نقدینگی مجوعه‌ای از توکن‌های قفل شده در قراردادهای هوشمند است که نقدینگی را در مبادلات غیر متمرکز به منظور کاهش مشکلات ناشی از عدم نقدینگی فراهم می‌کند.
4. CeFi

امور مالی متمرکز، واسطهای گران‌تری است هزینه‌های سنگین‌تری دارد.	نظام مالی غیرمتمرکز ارزان‌تر است، بیشتر هزینه‌های شبکه است.
امور مالی متمرکز می‌تواند سانسور شود.	نظام مالی غیرمتمرکز در مقابل سانسور مقاوم است.

تفاوت‌های اقتصاد غیر متمرکز[1] و بانکداری باز[2]

زمانی‌که در مورد بانکداری باز صحبت می‌کنیم، منظور سیستم بانکی است که در آن امکان دسترسی ایمن شخص ثالث به اطلاعات مالی از طریق آ.پی.آی‌ها[3] فراهم می‌گردد. این سیستم به اتصال داده و حساب‌ها بین مؤسسات مالی و بانک‌ها کمک می‌کند. همچنین به انواع جدید از کالاها و خدمات در سیستم مالی مرسوم اجازه می‌دهد. از سوی دیگر، نظام مالی غیرمتمرکز سیستم مالی کاملاً جدیدی عاری از زیرساخت کنونی ارائه می‌دهد. گاهی اوقات از اقتصاد غیرمتمرکز به‌عنوان اقتصاد باز[4] یاد می‌شود.

برای مثال، درحالی‌که بانکداری باز می‌تواند نظارت بر تمام ابزارهای مالی مرسوم را با یک اپلیکیشن و از طریق گرفتن اطلاعات از بانک‌ها و مؤسسات مختلف به‌صورت امن اجازه دهد؛ اما از سوی دیگر، نظام مالی متمرکز، می‌تواند نظارت از ابزارهای مالی کاملاً جدید و روش‌های جدید ارتباط با آن‌ها را اجازه دهد.

شما می‌توانید از نظام مالی غیرمتمرکز با نام پولی لگویی[5] نیز یاد کنید چرا که شما می‌توانید برنامه‌های غیرمتمرکز[6] را برای افزایش بازده‌تان روی هم انباشته کنید. برای مثال شما می‌توانید یک ارز ثابت[7] مانند دای را خریداری کنید سپس آن را تنها برای هدف کسب سود در کامپاند[8] وام بدهید. حقیقت جالب این است که شما تا زمانی که گوشی تلفن هوشمند خود را دارید نیازی به جست‌وجو برای ابزارهای جدید ندارید و بنابراین آماده هستید.

اگرچه بیشتر برنامه‌های غیرمتمرکز امروزی تخصصی و مناسب هستند، باز هم این امکان

---

1. DeFi (Decentralized Financial)
2. Open Banking
3. APA
4. Open Finance
5. Lego money
6. dApps

۷. Stable-coin این نوع ارز کلاس جدیدی از ارزهای رمز پایه است که سعی در ارائه ثبات قیمت دارد و توسط یک دارایی ذخیره پشتیبانی می‌شود.

۸. Compound یک پروتکل نرخ بهره‌ی الگوریتمی و مستقل است.

هست که برنامه‌های[1] آینده بتوانند زندگی و فعالیت‌های روزمره را تحت‌تأثیر قرار دهند. به‌عنوان مثال شما در یک برنامه نظام مالی غیرمتمرکز و بر اساس یک قرارداد رهن قادر خواهید بود ماشین یا خانه بخرید و باید در زمان تعیین‌شده‌ای (چند ماه یا چند سال) بازپرداخت کنید. اسناد و مدارک به شکل توکن‌شده در یک حافظه بلاکچین به‌عنوان وثیقه قرار می‌گیرند و اگر شما به هر شکلی بازپرداخت خود را متوقف کنید، اسناد و مدارک به‌صورت طبیعی به صاحب جدید منتقل شده که وام‌دهنده است و به او تعلق خواهد داشت. با توجه به مفهوم بانک‌ها و وکلا، تمام فرایند خرید و فروش ماشین یا خانه ارزان‌تر می‌شود.

چرا هایپ؟

نخست، نظام مالی غیرمتمرکز توانسته در این فضا نسبت به سایر تنظیم‌کننده‌های عقب‌تر از خود برتری داشته باشد؛ به‌عنوان مثال در وام‌های بدون وثیقهٔ مرسوم، نیاز به قانونی بودن وجود دارد که در آن وام‌دهنده و وام‌گیرنده با یکدیگر آشنا می‌شوند (هویت یکدیگر را می‌دانند) و وام‌دهنده حق دارد برای اطمینان از تمایل برای بازپرداخت وامِ گرفته شده، وضعیت مالی وام‌گیرنده را ارزیابی کند؛ اما در نظام مالی غیرمتمرکز چنین الزاماتی نیاز نیست. در عوض تماماً در ارتباط با اعتماد و حفظ حریم خصوصی متقابل است.

اکنون تنظیم‌کننده‌ها باید برای محافظت از جامعه در مقابل ریسک‌هایی نظیر اینکه مردم پول خود را در فضایی که تنظیم نشده و یا بانک‌ها و سایر مؤسسات مالی که ظرفیت ایفای نقش به‌عنوان واسطه را ندارند، قرار دهند، تعادل شکننده[2] بین سرکوب نوآوری و شکست (پروژه) را اندازه‌گیری کنند. بااین‌حال به نظر می‌رسد همان‌گونه که امروزه شاهد آن هستیم، پذیرفتن تغییر، روش معقول‌تری برای ادامه است. کمیسیون بورس و اوراق بهادار ایالات متحده[3] با پذیرفتن نظام مالی غیرمتمرکز از طریق تصویب صندوق بر پایهٔ اتریوم[4]، به نام آرکا[5]، برای اولین‌بار در جولای سال ۲۰۲۰ میلادی تغییر بسیار مهمی ایجاد کرد.

چون یکی از بزرگترین چالش‌ها در مورد نوآوری مالی، محیط تهاجمی است که توسط تنظیم‌کننده‌های قدیمی برای دوران گذشته نوشته شده است، این تغییر بسیار مهم و مورد

1. applications
2. fragile balance
3. SEC
4. Ethereum-based fund
5. Arca

استقبال است. برخی از این مقررات منجر به عدم موفقیت چند پروژه نظام مالی غیرمتمرکز شد، از جمله یکی از مهم‌ترین‌های این پروژه‌ها، پایهٔ مستقر در نیوجرسی[1] است که در آنجا، در سال ۲۰۱۸ میلادی زمانی که عدم تطبیق با قوانین کمیسیون بورس و اوراق بهادار ایالات متحده نهایی شد، مبلغ ۱۳۳ میلیون دلار به سرمایه‌گذاران بازگردانده شد.

دوم، به دلیل پیدایش نظام مالی غیرمتمرکز، بازیگران جریان اصلی درگیر می‌شوند. بیشتر سازمان‌های مالی اصلی و مهم در حال شروع به تأیید نظام مالی غیرمتمرکز و به دنبال راه‌هایی هستند که در آن سهمی داشته باشند. به‌عنوان مثال تعداد ۷۵ بانک از بین بزرگترین بانک‌های دنیا در حال دنباله‌روی از تکنولوژی بلاکچین و آزمایش آن، برای افزایش سرعت پرداخت‌ها به‌عنوان بخشی از شبکه اطلاعات داخل بانکی هستند. این امر اولین بار توسط جی پی مورگان[2]، بانک و شرکت مالی آ.ان.زد[3] و رویال بانک کانادا[4] انجام شد.

همچنین صندوق‌های مدیریت دارایی مهم و قوی شروع به جدی گرفتن نظام مالی غیرمتمرکز کرده‌اند. مشهورترین مورد این گروه، گری‌اسکیل[5]، بزرگترین حساب سرمایه‌گذاری رمزنگاری‌شده (کریپتو) در جهان است. این شرکت بیش از ۵/۲ میلیارد دلار از سرمایهٔ رمزنگاری‌شده، از جمله ۴/۴ میلیارد دلار بیت‌کوین را مدیریت می‌کند.

سوم، تأثیر بیماری کووید ۱۹ است. این همه‌گیری جهانی، نرخ بهرهٔ جهانی را حتی به کمتر از قبل هدایت کرده است. برخی از مناطق مانند منطقه یورو[6] و مشابه، اکنون در حوزهٔ منفی قرار دارند. سایرین از جمله ایالات متحده و انگلیس اگر از سیاست‌های انبساطی پولی و مالی که برای مبارزه با افزایش نرخ بیکاری ناشی از کووید ۱۹ پیاده‌سازی شده، مراقبت نکنند می‌توانند نفرات بعد باشند.

در چنین شرایطی، نظام مالی غیرمتمرکز بازده بسیار بالاتری نسبت به سازمان‌های مالی مهم و اصلی به پس‌اندازکنندگان ارائه می‌دهد. به‌عنوان مثال، کامپاند نرخ بهره سالانه ۶٫۷۵ درصد را برای کسانی که با ارز ثابت تتر[7] پس‌انداز کرده‌اند ارائه داده است. در این حالت نه‌تنها سود پس‌انداز خود را دریافت می‌کنید بلکه باید گیرنده توکن کامپاند نیز باشید که این خود یک

1. New-Jersey-based Basis
2. JP Morgan
3. ANZ
4. Royal Bank of Canada
5. Grayscale
6. Eurozone
7. Tether

جذابیت بیشتر و انگیزه مضاعف است. با استفاده از نظام مالی غیرمتمرکز، لازم نیست نگران داشتن حساب بانکی باشید، یک تلفن هوشمند در اختیار داشته باشید تا منابع مالی در یک ظرف طلا به شما ارائه شود.

سرانجام افرادی که پول خود را در توکن‌های نظام مالی غیرمتمرکز می‌گذارند، افزایش یافته است. زیرا مردم از عقب ماندن امتناع می‌کنند و نمی‌توانند توانایی رشد نمایی خود را انکار کنند. این روزها شاهد هیجان نامعقول زیادی هستیم، زیرا مشاهده می‌شود بسیاری از توکن‌ها هیچ ارزشی یا تقریباً هیچ ارزشی ندارند. چه موافق باشید و چه نباشید، ما به سمت دستیابی به موفقیت جدید مالی پیش رفته‌ایم که آزادتر و غیرمتمرکزتر از هر زمان دیگری است. سؤال بزرگ این است: چگونه می‌توانیم توسعه آن را با کنترل و تعادل هدایت کنیم تا خطرات را کاهش داده و مزایای احتمالی را به‌طور گسترده‌تر پخش کنیم؟ این چالشی است که ثمرهٔ کار را در چند سال آینده تهدید می‌کند.

مزایای نظام مالی متمرکز:

امور مالی غیرمتمرکز از استانداردهای اصلی بلاکچین اتریوم استفاده می‌کند تا امنیت و شفافیت مالی، نقدینگی باز و فرصت‌های رشد و رضایت از یک سیستم اقتصادی یکپارچه و سازمان یافته را به حداکثر برساند.

قابلیت برنامه‌ریزی[1]

قراردادهای هوشمند بسیار قابل برنامه‌ریزی هستند و عملکرد را به‌طور خودکار انجام می‌دهند و ابزارهای مالی جدید و سرمایه‌گذاری‌های دیجیتالی را تشویق می‌کنند.

تغییر ناپذیری[2]

هم‌افزایی داده‌هایی که مقاوم در برابر تغییر[3] هستند، در بین ساختارهای غیرمتمرکز بلاکچین، باعث افزایش ایمنی و قابلیت شنیده شدن می‌شود.

قابلیت همکاری[4]

پشته[5] نرم‌افزار قابل مقایسه اتریوم، اطمینان می‌دهد که خط مشی‌ها و برنامه‌های نظام مالی

1. Programmability
2. Immutability
3. Change-proof data
4. Interoperability
5. Stack

غیرمتمرکز برای ترکیب و تکمیل یکدیگر طراحی شده‌اند. توسعه‌دهندگان[1] (نرم‌افزاری) برای ایجاد آن در موقعیتی فراتر از سیاست‌های موجود، رابط‌های[2] سفارشی و برنامه‌های یکپارچه ثالث با نظام مالی غیرمتمرکز از انعطاف‌پذیری لازم برخوردار هستند. ازاین‌رو، مردم اغلب از آن به‌عنوان پول لگویی یاد می‌کنند.

شفافیت

تمام تراکنش‌ها توسط کاربران شبکه عمومی بلاکچین اتریوم پخش و تایید می‌شوند. توجه به این نکته مهم است که آدرس‌ها در اتریوم رمزگذاری شده هستند که شبه ناشناس می‌باشند. میزان شفافیت تراکنش‌های داده به دلیل بینش غنی داده‌ها و در دسترس بودن زیاد شبکه‌ای که در تمام طول سال و بدون توقف در دسترس است، بسیار مطلوب است. خط مشی‌های اجرایی بر روی اتریوم و نظام مالی غیرمتمرکز نیز با کد باز[3] برای مشاهده، ممیزی و ایجاد در دسترس همه قرار دارد.

بدون مجوز بودن

برخلاف منابع مالی مرسوم، ویژگی نظام مالی غیرمتمرکز، باز بودن آن است و نیازی به اجازه دسترسی ندارد. هرکسی که دارای کیف پول رمزنگاری‌شده و یک اتصال اینترنت باشد، می‌تواند بدون توجه به موقعیت مکانی خود و اغلب بدون انتظار هرگونه کاهشی در مقدار وجه به برنامه‌های نظام مالی غیرمتمرکز در اتریوم دسترسی پیدا کند.

خود مراقبتی[4]

استفاده از یک کیف پول وب تری[5] مانند متاماسک[6] برای برقراری ارتباط با برنامه‌ها و سیاست‌های مالی غیرمجاز، باعث می‌شود طرفین در نظام مالی غیرمتمرکز همیشه دارایی داده‌ها و تنظیم‌گری خود را کنترل کنند.

امتیازهای نظام مالی متمرکز

معمولا امور مالی به بانک‌ها بابت عمل به‌عنوان واسطه‌گر و دادگاه‌ها برای قضاوت در صورت نیاز بستگی دارد. با وجود این، برنامه‌های نظام مالی غیرمتمرکز نیازی به داور یا واسطه‌گر

1. developers
2. interface
3. Open source code
4. Self-custody
5. web3
6. MetaMask

ندارند. این امر به این خاطر است که کد مورد نظر، راه‌حل هر اختلافی که احتمال رخداد آن وجود دارد را ارائه داده و دیکته می‌کند و کاربران از کنترل صحیح وجوه خود به‌صورت تمام وقت اطمینان حاصل می‌کنند. این روش هزینهٔ مربوط به ایجاد و استفاده از این محصولات را کاهش داده و جای خود را به یک عملیات مالی بدون تنش می‌دهد.

لحظه‌ای که این سرویس‌های مالی جدید بر روی بلاکچین نصب می‌شود، نقاط خرابی منحصربه‌فرد خارج می‌گردند. سپس داده‌ها بر روی بلاکچین مستند شده و در چندین نود (ایستگاه) منتشر می‌شوند و احتمال توقف سرویس را از بین می‌برد که کار چندان آسانی هم نیست. حقیقت این است که چهارچوب‌هایی برای برنامه‌های نظام مالی غیرمتمرکز می‌توان از قبل ایجاد کرد که البته با استفاده از شرایط، کمتر پیچیده و ایمن‌تر خواهد بود.

از دیگر مزایای مهم چنین اکوسیستم قابل دسترسی، سادگی دسترسی برای کاربرانی است که به‌صورت معمولی دسترسی به خدمات مالی ندارند. از آنجا که سیستم مالی معمول برای کسب سود به واسطه‌ها بستگی دارد، خدمات آن‌ها معمولاً در مناطقی با درآمد کم وجود ندارد؛ بااین‌حال، هزینه‌های نظام مالی غیرمتمرکز به‌طور عمده کاهش یافته و فردی با درآمد پایین نیز می‌تواند از این دامنه خدمات مالی، سریع‌تر بهره‌مند شود.

نظام مالی غیرمتمرکز و ریسک‌های احتمالی

نظام مالی غیرمتمرکز هر چقدر هم خوب به نظر برسد با چالش‌هایی روبه‌رو است که باید درباره‌اش با افرادی که احتمالاً به آن علاقه‌مندند، بحث شود. این کار برای این است که شما را از آنچه با آن درگیر هستید، به‌درستی آگاه کند.

قبل از جلو رفتن در این بخش اشاره به خطرات احتمالی نظام مالی غیرمتمرکز نیز دارای اهمیت است. از بزرگترین ریسک‌ها، خطاها، اشکالات و آسیب‌پذیری موجود در قراردادهای هوشمند تغییر پروتکل است که می‌تواند قراردادهای موجود را تحت‌تأثیر قرار دهد. به همین دلیل، استفاده‌کنندگان برای کاهش خطر مشکلات احتمالی به (نوعی) بیمه اضافی نیاز دارند. همچنین همیشه باید بررسی کنید که پروژه نظام مالی غیرمتمرکز شما چقدر غیرمتمرکز است و در صورت بروز اشتباه، روند متوقف کردن چیست.

ممکن است یک فرد دارای یک کلید ادمین باشد که می‌تواند پروتکل را غیرفعال کند،

یا امکان دارد یک سیستم مدیریت بدون تماس[1] وجود داشته باشد که چنین تصمیماتی را می‌گیرد. همچنین اگر همیشه خطرهای سیستماتیک‌تری را در نظر داشته باشید که ممکن است ناشی از مثلاً کاهش بهای ناگهانی قیمت یک دارایی باشد، یاری‌رسان خواهد بود. این می‌تواند منجر به نقدینه‌سازی زنجیره‌ای از طریق چندین پروتکل نظام مالی غیرمتمرکز شود. بار شبکه و ازدحام نیز می‌تواند یک مسئله باشد. این امر به‌ویژه اگر از تصفیه (انحلال) جلوگیری کرده و سعی در تأمین امنیت به موقع داشته باشد، درست است.

راه‌حل‌های مقیاس‌پذیر آینده اتریوم ۲.۰ و تیر۲[2] می‌توانند به حل این مشکل کمک کنند. این برنامه همچنین دارای ویژگی‌های ظریف و تغییراتی است که به یکی از پروتکل‌ها اعمال می‌شود و باعث می‌شود کاربران اقداماتی را که منجر به رخدادِ پی‌درپی می‌شود، از طریق پروتکل‌های مختلف با وضوح کمتری انجام دهند. یک مثال خوب در این مورد افزایش اخیر ترکیب پروتکل‌های کامپاند است که استفاده‌کنندگان را مجبور به گرفتن وام‌های به‌ظاهر بدون سود با نرخ بهرهٔ بالا کرد که به دلیل جبران خسارت اضافی کامپاند سودآور بود. این شرایط می‌تواند بسیار خطرناک باشد، اما همان طور که متوجه شده‌اید کل اکوسیستم را قدرتمندتر کرده است و نسبت به شرایط مشابه در آینده، حساسیت را کمتر می‌کند.

نظام مالی غیرمتمرکز، یک فضای جذاب و پُرجنب‌وجوش و پر از فرصت است، اما مهم است به خاطر داشت هنوز یک صنعت نسبتاً جدید و نوظهور است؛ بنابراین بازی است که ریسک بالا و درآمد بالایی دارد. نظام مالی غیرمتمرکز، برخلاف بیشتر شرکت‌های فناوری تقریباً یک آشفتگی واقعی برای صنعت مالی سنتی محسوب می‌شود. نظام مالی غیرمتمرکز بر اساس تکنیک‌ها و رویه‌های قدیمی نیست و بر پایهٔ روش‌های جدید است.

در حال حاضر بیشتر محصولات مالی فقط توسط بانک‌ها ساخته می‌شود. نظام مالی غیرمتمرکز، منبع باز[3] است و به احراز هویت احتیاج ندارد و همکاری مشابه اینترنت را ممکن می‌سازد. نظام مالی غیرمتمرکز اساساً بر پایهٔ اتریوم است که از پروتکل‌های قابلیت همکاری بیشتری استفاده می‌کند. اما در آینده خواهیم دید که پروژه‌های بیشتری روی زنجیره‌های (چین‌های) مختلف ساخته خواهند شد.

در اینجا برخی از آن‌ها به صورت پررنگ نشان داده شده‌اند:

---

1. Contactless management system
2. Tier
3. Open source

- **عملکرد ضعیف**

بلاکچین به‌طور طبیعی کندتر از شرکای متمرکز خود است و به برنامه‌های اجرا شده بر آن نیز تسری داده شده است. بنابراین توسعه‌دهندگان برنامه نظام مالی غیرمتمرکز، نیاز دارند این محدودیت را یادداشت کرده و محصولات خود را بر این اساس بهبود بخشند.

- **خطاهای کاربران**

این مسئولیت از طریق واسطه‌ها توسط برنامه‌های نظام مالی غیرمتمرکز به کاربران منتقل می‌شود. این بدان معناست که شما به دلیل کمبود اختیارات مرکزی، کاملاً توسط خودتان کنترل می‌شوید که به‌سرعت می‌تواند برای بسیاری از کاربران (اثر) منفی داشته باشد. طراحی یک محصول با ریسک کم یا داشتن حداقل خطاهای کاربر، مشخصاً یک چالش سخت برای موفقیت است، مخصوصاً زمانی‌که محصول روی بلاکچینی سفت و چسبنده[1] قرار داده شده است.

- **تجربه کاربر بد**

در حال حاضر استفاده از برنامه‌های نظام مالی غیرمتمرکز به تلاش بیشتر کاربر نیاز دارد. برنامه‌های نظام مالی غیرمتمرکز باید یک مزیت قابل توجه داشته باشند که باعث ایجاد انگیزه و تشویق کاربران برای تغییر شیوه‌های معمول سیستم شود. این امر به آن‌ها برای تبدیل به یک جز مرکزی از سیستم مالی بین‌المللی کمک می‌کند.

- **اکوسیستم آشفته**

یافتن یک برنامه عالی و مناسب برای یک مورد خاص می‌تواند کاملاً چالش‌برانگیز باشد. بااین‌حال کاربران باید برای کشف بهترین سناریوها در هر زمان وقت و توانایی داشته باشند. این مشکل فقط هنگام ساخت برنامه‌ها ایجاد نمی‌شود، بلکه زمانی که به این فکر می‌کنیم چطور آنها را در یک اکوسیستم نظام مالی غیرمتمرکز و گسترده‌تر هماهنگ کنیم، نیز وجود دارد.

1. Rigid blockchains

فصل ۵

کشت سود (ییلد فارمینگ) در امور مالی غیرمتمرکز به چه معناست؟

با ادامه پیشرفت بخش جدید و مهیج مالی، تمایل مصرف‌کنندگان برای مشارکت در رشد پروتکل افزایش یافته است. چه اینکه آن را به همان سادگیِ معرفی ارز دیجیتال برای کامپاند و چه در ازای یک چیز پیچیده‌تر مثل مشارکت در مزایدهٔ نقدینگی میکر[1] تلقی کنیم، به‌هرحال امور مالی غیرمتمرکز فرصت‌های جدید و مهیج در زمینهٔ کسب درآمد منفعلانه ایجاد می‌کند.

روش کسب سود در حال تکامل و راستی‌آزمایی است اما پیامدهای آن شگفت‌انگیز است. در اینترنت عمومی نمی‌توان محصولی را خرید مگر اینکه اطلاعات کافی مورد نیاز جهت فعال‌سازی تراکنش را به صاحب وب‌سایت بدهید. اما با وجود امور مالی غیرمتمرکز، شما می‌توانید پول قرض کنید بدون اینکه حتی نام یا اطلاعات شخصی خود را فاش کنید. اپلیکیشن امور مالی غیرمتمرکز اهمیتی نمی‌دهد؛ زیرا وثیقه‌ای برای تأمین بدهی ارائه می‌کند (برای مثال در بستر نرم‌افزار کامپاند، وام ده دلاری به وثیقه‌ای (تضمینی) به ارزش حدود بیست دلار نیاز دارد).

اگر این توصیه را دنبال می‌کنید و تصمیم به تجربه کردن و آزمایش آن گرفتید، می‌توانید به‌محض انجام کار آن را به حالت قبل برگردانید، شاید بتوان گفت بعد از ده دقیقه، این کار شدنی است؛ بااین‌حال، تجربه خوبی است برای کسی که در مورد مزایای منحصربه‌فرد پیشنهادات کشت سود، کنجکاو است.

بنابراین چرا به افرادی که پول دارند وام می‌دهند؟ اغلب این کار را به‌منظور نوعی معامله

---

1. Maker›s liquidation auction

انجام می‌دهند. واضح‌ترین مثال، فروش استقراضی[1] در بازار (کسب سود به هنگام افت قیمت) است. همچنین برای افرادی که قصد دارند توکن‌های خود را سپرده کنند و درعین‌حال به خریدوفروش در بازار نیز مشغول باشند، این کار عالی است.

آیا برای راه‌اندازی یک بانک به پول زیادی نیاز ندارید؟

درست است! در امور مالی غیرمتمرکز، تأمین این پول در ابتدا از غریبه‌ها در اینترنت انجام می‌گیرد. به همین دلیل، روشی هوشمندانه برای برنامه‌های غیرمتمرکز بانکی به‌منظور جذب نگه‌دارندگان ارزهای دیجیتال[2] برای طولانی مدت است.

مسئله اساسی تمام این محصولات، نقدینگی است. به عبارت دیگر چه میزان منابع مالی در قرارداد هوشمند سپرده‌گذاری شده است؟ برای برخی از انواع محصول، تجربه محصول با نقدینگی بهترین حالت را دارد. آویچال گارگ[3]، شریک ارشد شرکت الکتریک کپیتال[4] می‌گوید:«آن‌ها به‌جای قرض گرفتن از سرمایه‌گذاران خطرپذیر (ریسک‌پذیر) یا سرمایه‌گذاران بدهی، از مصرف‌کنندگان قرض می‌گیرند.» برای مثال از یونی سواپ[5] استفاده کنید. یونی سواپ از بازار ساز خودکار یا همان آ.ام.ام حمایت و طرفداری می‌کند. (اصطلاح دیگر برای هنر نظام مالی غیر متمرکز[6]). به‌طور خلاصه یونی سواپ یک سیستم رباتیک تحت وب است که دائماً در حال خریدوفروش هر کوین رمزنگاری‌شده در بازار است.

یونی سواپ تقریباً برای هر توکن اتریوم یک یا چند جفت معاملاتی[7] دارد. در پشت صحنه، این بدان معناست که یونی سواپ می‌تواند وانمود کند که مستقیماً دو توکن خریدوفروش می‌کند. انجام این کار برای مصرف‌کنندگان آسان‌تر است اما همه‌چیز بر اساس یک استخر با دو توکن است و هرکدام از این جفت معاملاتی(بازاری) در یک استخر بزرگتر عملکرد بهتری دارند.

استخرها به چه معنا هستند؟

بیایید نگاهی به نحوهٔ کار یونی سواپ بیندازیم تا نشان دهیم چرا مقدار پول بیشتر کمک‌کننده

1. Shorting
2. empty HODLers
3. Avichal Garg
4. Electric Capital
5. Uniswap
6. DeFi art
7. Marketing pairs

است. وجود بازاری برای دای و یو.اس.دی.سی، سکه دلار آمریکا را در نظر بگیریم. هر دو توکن، استیبل کوین هستند و ارزشی برابر ۱ دلار دارند اما مکانیسم‌های مختلفی برای ذخیره ارزش خود دارند. این امر معمولاً در هریک از توکن‌ها اتفاق می‌افتد.

قیمتی که یونی سواپ برای هر توکن در یک جفت معاملاتی مجزا نشان می‌دهد، بر اساس موجودی هر توکن در استخر تعیین می‌شود؛ به عنوان مثال اگر نیاز به ایجاد استخر یو.اس.دی.سی/ دای باشد، برای ساده‌سازی آن‌ها، باید مقادیر یکسانی از هر دو سپرده‌گذاری شود. برای استخری با ۲ یو.اس.دی و ۲ دای، قیمت برای هر دای معادل ۱ دلار است. اما تصور کنید کسی ۱ دای سپرده کند و ۱ دلار برداشت کند. اکنون ۱ یو.اس.دی و ۳ دای در استخر وجود خواهد داشت. استخر به ترتیب خوب و مناسب خواهد بود. سرمایه‌گذاران با تجربه می‌توانند با سرمایه‌گذاری ۱ دلار به‌راحتی نیم دلار درآمد کسب کنند و همچنین ۱,۵ دای به دست آورند. این کار معادل ۵۰ درصد آربیتراژ بوده و یک مسئله نقدینگی محدود به‌شمار می‌رود.

ضمناً به همین دلیل است که قیمت‌های یونی سواپ معمولاً صحیح هستند. همچنین معامله‌گران در بازارهای بزرگ‌تر برخی انحرافات قیمتی را پیدا می‌کنند و در جهت کسب منافع حاصل از آربیتراژ به‌سرعت وارد معامله می‌شوند. بااین‌حال، اگر موجودی استخر ۵۰۰۰۰۰ یو.اس.دی.سی در برابر ۵۰۰۰۰۰ دای باشد، مبادله ۱ دای در برابر ۱ یو.اس.دی.سی تأثیر ناچیزی بر قیمت نسبی دارد. به همین دلیل است که نقدینگی بالا بسیار مفید و تأثیرگذار است. دارایی‌ها را می‌توان برای کسب سود اندکی در پلتفرم کامپاند قفل کرد. به نظر می‌رسد کشت سود، گروه گسترده‌تری از سرمایه‌گذاران خرد را به خود جلب می‌کند و سرمایه‌گذاران حرفه‌ای که به دنبال راهکارهایی برای به حداکثر رساندن سود خود هستند، همان کسانی‌اند که به کشت سود می‌پردازند.

امور مالی غیرمتمرکز اثرات مرتبط ایجاد می‌کند، بنابراین بازار به نقدینگی اضافه نیاز دارد. یونی سواپ این مشکل را با شارژ یک هزینهٔ اندک برای هر تراکنش برطرف می‌کند. یونی سواپ با کاهش اندکی از هر تراکنش و قراردادن آن در استخر، این مشکل را حل می‌کند. (چون دای بعد از دریافت کارمزد یا کمیسیون با قیمت ۰,۹۹۷ دلار مبادله می‌شود، مجموع استخر ۰,۰۰۳ دلار افزایش می‌یابد). این امر کمک می‌کند هنگامی که فردی نقدینگی را وارد می‌کند، تأمین‌کنندگان نقدینگی سهمی از استخر داشته باشند و چنانچه در این استخر تراکنش زیادی صورت بگیرد، کارمزد بیشتری دریافت می‌شود و ارزش استخر نقدینگی افزایش می‌یابد که به‌صورت توکن بازگردانده می‌شود. نقدینگی اضافه شده به یونی سواپ به‌صورت توکن

نشان داده می‌شود. نه اینکه به‌صورت یک حساب نمایش داده شود. کشت سود ارز دیجیتال راهی برای تولید کوین‌های رمزنگاری‌شده بیشتر توسط یک ارز دیجیتال دیگر است. این کار تماماً به استفاده کردن از اپلیکیشن‌های امور مالی غیرمتمرکز برای وام دادن (قرض دادن) بستگی دارد. منظور وام دادن به افرادی است که از مراحل از پیش تعیین‌شده در یک قرارداد هوشمند استفاده می‌کنند. شما به ازای خدمات خود کارمزدی به‌صورت ارز دیجیتال دریافت می‌کنید. این کار بسیار ساده به نظر می‌رسد، این‌طور نیست؟ خب، آن‌طور که فکر می‌کنید نیست.

کشت‌کنندگان موفق سود از سیستم‌ها و استراتژی‌های بسیار پیچیده استفاده می‌کنند. آن‌ها به‌طور مرتب کوین‌های رمزنگاری‌شده را به‌منظور افزایش سود بین بازارهای مختلف جابه‌جا می‌کنند. آن‌ها همچنین در مورد بهترین استراتژی‌های به کار برده شده در کاشت بسیار محرمانه رفتار می‌کنند. چرا؟ هرچه بیشتر استراتژی خود را نشان دهند تأثیر آن کمتر می‌شود.

کشت سود، برابر با نمودارهای جنگلی یا نمودارهای انباشت[1] در امور مالی غیرمتمرکز سرزمین است. در واقع جایی است که کشت‌کنندگان (کشاورزان) در حال رقابت برای پرورش بهترین محصولات هستند. جنبش امور مالی غیرمتمرکز در خط مقدم نوآوری در بلاکچین بوده است. چه چیزی اپلیکیشن‌های امور مالی غیرمتمرکز را این‌گونه خاص می‌کند؟ اینکه آن‌ها مجاز نیستند و مصوبه‌ای ندارند؛ بنابراین هرکسی با دسترسی به یک ارتباط اینترنتی و یک کیف پول ثانویه می‌تواند با آن‌ها ارتباط برقرار کند. این برنامه‌ها نیاز به متولی یا کارگزاران را از بین می‌برد. وقتی می‌توانم دارایی را مجبور به کار کردن کنم، چرا به‌طور غیرفعال از آن استفاده کنم؟ پس کشت‌کنندگان با بهره‌وری بالا چگونه سود خود را به دست می‌آورند؟ در زیر همه را توضیح خواهم داد.

کشت سود: توضیح اجمالی

کشت سود سودآور یا همان طور که گفته شد استخراج نقدینگی از ارز رمزنگاری‌شده در جهت کسب سود بهره می‌برد. به بیان ساده، این به معنای سپردن (استیکینگ) کوین‌ها و دریافت سود از مقادیر ذخیره‌شده (استیک‌شده) است.

به تعبیری این فرآیند از نظر ماهیت بسیار شبیه سپرده‌گذاری کوین‌ها است؛ اما با وجود بسیاری موانع (پیچیدگی‌های) پس‌زمینه‌ای، متفاوت عمل می‌کند. غالباً کاربران به‌عنوان

1. Forest plots

تأمین‌کنندگان[1] شناخته می‌شوند که نقش بزرگی در افزودن نقدینگی به استخر نقدینگی دارند.

استخر نقدینگی صرفاً یک قرارداد هوشمند با پول سپرده‌گذاری شده است. به تأمین‌کنندگانِ نقدینگی، بابت فراهم‌آوری نقدینگی برای استخر، جبرانی داده می‌شود. پاداش‌ها را می‌توان از طریق کارمزدهای به دست آمده تحت پلتفرم نظام مالی غیرمتمرکز یا از منابع دیگر به دست آورد.

پاداش برخی از استخرهای نقدینگی با چندین توکن مختلف داده می‌شود. توکن‌های پاداش در استخرهای نقدینگی دیگر سپرده‌گذاری می‌شوند که خود می‌تواند پاداش کسب کند. اکنون می‌توانید ببینید که یک استراتژی فوق‌العاده پیچیده با چه سرعتی پدید می‌آید. بااین‌حال، ایده اصلی این است که تأمین‌کنندگان نقدینگی در منابع نقدینگی سرمایه‌گذاری می‌کنند و در ازای آن پاداش می‌گیرند.

کشت سود معمولاً با توکن‌های استاندارد ای.آر.سی ۲۰اتریوم[2] انجام می‌شود و پاداش‌ها نیز به‌طورکلی از نوع توکن ای.آر.سی۲۰ است. بااین‌حال، ممکن است در آینده تغییر کند. چرا؟ چون در حال حاضر، بیشتر این فعالیت‌ها در اکوسیستم اتریوم انجام می‌شود. بااین‌حال، ارتباطات میان زنجیره‌ای[3] و سایر پیشرفت‌های مشابه می‌تواند باعث شود برنامه‌های نظام مالی غیرمتمرکز، در آینده از پلتفرم‌های تحت بلاکچین جدا شوند. این بدان معناست که هر قرارداد هوشمند با هر بلاکچین دیگری سازگار است که از قابلیت‌های آن قرارداد پشتیبانی می‌کند.

کشت‌کنندگان به‌طور معمول منابع خود را در جست‌وجوی بازدهی بالا بین پروتکل‌های متفاوت جابه‌جا می‌کنند. در نتیجه پلتفرم نظام مالی غیرمتمرکز می‌تواند مشوق‌های مالی دیگری را نیز برای جذب سرمایه بیشتر، به این سیستم فراهم کند. مشابه بورس سهام مرکزی، نقدینگی سبب جذب نقدینگی بیشتر می‌شود.

چه چیزی آغازگر رونق محصول بود؟ علاقه ناگهانی به کشت سود می‌تواند با راه‌اندازی توکن کامپاند مرتبط باشد که یک توکن پیچیدهٔ مدیریت اکوسیستم مالی است. توکن کنترل به دارنده، حق اداره آن را می‌دهد. اما چگونه این توکن‌ها را توزیع می‌کنید که شبکه تا حد ممکن غیرمتمرکز شود؟ یک روش معمول برای راه‌اندازی بلاکچین غیرمتمرکز، توزیع این توکن‌های کنترل به‌صورت الگوریتمی به‌عنوان مشوق‌های نقدینگی است. این بدان معنی است که تأمین‌کنندهٔ نقدینگی، توکن جدید را کشت و نقدینگی پروتکل را تأمین می‌کند.

---

1. LPs
2. Ethereum›s ERC-20
3. Cross-chain Blockchain

اگرچه این شرکت کشت سود را اختراع نکرده است، اما انتشار کامپاند باعث شهرت بیشتر این نوع مدل توزیع ارز رمزنگاری‌شده گردیده است. بعد از آن، سایر پروژه‌های نظام مالی غیرمتمرکز، طرح‌های ابتکاری را در جهت ورود نقدینگی به اکوسیستم ارائه داده‌اند.

ارزش کل قفل‌شده[1] یا همان تی.وی.ال چیست؟

بهترین روش برای اندازه‌گیری سلامت مزرعه نظام مالی غیرمتمرکز، نظارت بر شاخص ارزش کل قفل‌شدهٔ تی.وی.ال است. این شاخص نشان می‌دهد چه مقدار ارز دیجیتال در پلتفرم وام‌دهی و یا در سایر بازارهای ارز دیجیتال قفل شده است. به عبارتی، تی.وی.ال، کل نقدینگی استخر نقدینگی است. این شاخص، یک معیار مفید برای اندازه‌گیری سلامت نظام مالی غیرمتمرکز و به‌طورکلی بازار مزرعه کشت است. همچنین یک معیار مؤثر برای مقایسهٔ «سهم بازار» در پروتکل‌های مختلف نظام مالی غیرمتمرکز است. پالس (نبض) نظام مالی غیرمتمرکز، یک مکان عالی برای ردیابی تی.وی.ال است. می‌توانید ببینید کدام پلتفرم‌ها بیشترین دارایی اتریوم و یا سایر دارایی‌های رمزگذاری‌شدهٔ ذخیره در نظام مالی غیرمتمرکز را دارند. این مکان، یک نمای کلی از وضعیت فعلی کشت سود را ارائه می‌دهد. به‌طور طبیعی، ارزش ذخیره‌شدهٔ بیشتر، منجر به عملکرد بالاتر کشت سود می‌شود. می‌توانید ارزش تی.وی.ال را با اتریوم، یو.اس.دی یا حتی بیت‌کوین بی.تی.سی تخمین بزنید. هریک دیدگاه متفاوتی از وضعیت بازار پول نظام مالی غیرمتمرکز ارائه می‌دهند.

کشت سود چگونه اتفاق می‌افتد؟

کشت سود، ارتباط نزدیکی با مدل بازارساز خودکار دارد. به‌طور معمول شامل تأمین‌کنندگان نقدینگی و استخرهای نقدینگی می‌شود. تأمین‌کنندگان نقدینگی پول خود را در استخرهای نقدینگی سرمایه‌گذاری می‌کنند. این استخر بستری برای مبادله ایجاد می‌کند که در آن کاربران می‌توانند در وام گرفتن، وام دادن یا مبادلهٔ توکن‌ها اقدام کنند. استفاده از این پلتفرم‌ها به‌عنوان کارمزد محاسبه و بر اساس سهم (میزان مشارکت) تأمین‌کننده مالی در منابع نقدینگی پرداخت می‌شود.

با این‌همه، این عملیات می‌تواند متفاوت باشد. این یک فناوری جدید است و بی‌شک

1. Total Value Locked

رویکرد جدیدی در جهت بهبود عملکرد موجود مشاهده خواهید کرد. مشوق دیگر برای افزودن پول نقد به منابع نقدینگی در کنار کارمزد، می‌تواند توزیع توکن جدید باشد. به‌عنوان مثال، در بازار آزاد نمی‌توان ارز دیجیتال را در مقیاس کم خریداری کرد اما با تأمین نقدینگی در استخرهای مشخص به دست می‌آید. تمام قوانین توزیع بستگی به نحوهٔ اجرای منحصربه‌فرد پروتکل دارد. تأمین‌کنندگان نقدینگی بسته به میزان مشارکت در تأمین نقدینگی در استخر، کسب درآمد می‌کنند.

منابع سپرده‌گذاری معمولاً از انواع استیبل کوین‌ها با پشتوانه دلار هستند، بااین‌حال می‌تواند متفاوت باشد، برخی از استیبل کوین‌هایی که اغلب در امور مالی غیرمتمرکز مورد استفاده قرار می‌گیرند شامل دای، تتر، یو.اس.دی.تی، سکه دلار آمریکا، بیت‌کوین (بی.یو.اس.دی) و غیره هستند. برخی از پروتکل‌ها شامل کوین‌هایی می‌شوند که در یک قرارداد هوشمند یا در سیستم سپرده‌گذاری شده‌اند. به‌عنوان مثال، اگر دای را به کامپاند اضافه کنید، کامپاند دای یا «سی.دای» دریافت خواهید کرد. اتریوم را وارد کامپاند کنید، آنگاه شما، «سی. اتریوم» دریافت خواهید کرد.

این امر در چندین سطح قابل اجراست. می‌توان سی.دای را به پروتکل دیگری ارسال کرد که توکن دیگری به نمایندگی از سی.دای که نشان‌دهنده دای و غیره است، ارائه بدهد. این زنجیره‌ها می‌تواند بسیار پیچیده و دشوار باشد، اما می‌توانید یک روش ساده ۱:۱ را برای شروع دنبال کنید.

سودآوری کشت سود[1] چگونه تخمین زده می‌شود؟

سودآوری کشت سود معمولاً سالانه تخمین زده می‌شود. این مقدار تخمینی از مقدار مورد انتظار برای یک سال است. معمولاً به‌صورت نرخ سالانه[2] و بازده سالانه[3] اندازه گیری می‌شود. تفاوت آن‌ها این است که آ.پی.آر شامل بازده کامپاند نیست ولی شامل آ.پی.وای می‌شود. در کنار هم قرار دادن این دو به این معنی است که سود شما نیز یکراست سود بیشتری تولید می‌کند. با وجود این، آ.پی.آر و آ.پی.وای می‌توانند به‌جای هم استفاده شوند.

لازم به یادآوری است که این‌ها فقط تخمین و پیش‌بینی هستند. اندازه‌گیری درست سود

1. Yield Farming
2. APR
3. APY

در کوتاه مدت به دلیل رقابتی بودن و رشد سریع بازارها و تغییر سریع بازده‌ها دشوار است. اگر استراتژی برای برخی مواقع کار کند بسیاری از کشت‌کنندگان سود از فرصت استفاده می‌کنند و ممکن است ایجاد سودهای بیشتر را متوقف کنند.

از زمانی که آ.پی.آر و آ.پی.وای از بازارهای قدیمی آمده‌اند، ممکن است امور مالی غیرمتمرکز برای محاسبه درآمد به استفاده از آن نیاز داشته باشد. با توجه به‌سرعت امور مالی غیرمتمرکز، تخمین درآمد روزانه یا هفتگی می‌تواند منطقی‌تر باشد.

سیستم مالی غیرمتمرکز و سپرده‌های وثیقه

اگر تجارت کالا دارید، معمولاً باید برای گرفتن وام وثیقه فراهم کنید. این موضوع بیمه‌ای برای وام شما است. اما چگونه این قضیه به موضوع ما ربط پیدا می‌کند؟ بستگی دارد به پروتکلی که شما از طریق آن پول می‌پردازید که ممکن است نیاز باشد به سطح ریسک آن توجه کنید.

اگر ارزش وثیقه کمتر از آستانه مورد نیاز پروتکل شود، ممکن است حمایت از بازار آزاد از بین برود. برای جلوگیری از نقدینه‌سازی[1] آن، چه کاری می‌توان کرد؟ یک توکن اضافه کرد.

دوباره باید گفت که هر پلتفرم مجموعه‌ای از قوانین مخصوص به خود دارد که وثیقه‌ها به اجبار با هم در ارتباط هستند. همچنین ممکن است شما با مفهوم لانه‌سازی[2] یا وثیقه‌گذاری بیشتر[3] کار کنید. به این معنی که قرض‌گیرنده باید وثیقه‌ای بیشتر از مقداری بگذارد که وام می‌گیرد. در این حالت ریسک پایین آمدن ناگهانی قیمت در بازار را کم می‌کند، اگرچه احتمال از بین بردن مقدار زیادی وثیقه از سیستم را فعال می‌کند.

بنابراین باید بگوییم که برای پروتکل وام‌دهی باید ٪۲۰۰ وثیقه وجود داشته باشد. به این معنی که برای هر صد دلاری که دارید پنجاه دلار می‌توانید وام دریافت کنید. اگرچه در حالت کلی برای کاهش ریسک نقدینه‌سازی بهتر است که وثیقه بیشتری داشته باشید. بسیاری از سیستم‌ها نسبت تناسب بالاتری دارند (مثلاً ٪۷۵۰) به این خاطر که پلتفرم را در برابر ریسک نقدینه‌سازی محفوظ کنند.

1. liquidation
2. nesting
3. over-collateralization

خطرات ذاتی در کشت سود

موفقیت در کشت سود، کار ساده‌ای نیست. بیشتر استراتژی‌های رشد سود خیلی پیچیده‌اند و فقط برای کاربران پیشرفته توصیه می‌شود. همچنین کشت سود بیشتر برای افرادی مناسب‌تر است که مقدار زیادی از رمزنگاری‌شده‌ها را دارند که به «نهنگ ها[1]» معروف هستند.

باید بدانیم که چه کاری انجام دهیم که پول از دست ندهیم. علاوه بر ریسک نقدینه‌سازی وجوه سپرده‌گذاری‌شده، به ریسک دیگری بپردازیم که به کشت سود مربوط می‌شود. یکی از خطرات مشاهده شده برای کشت سود، قرارداد هوشمند است. به‌علت ماهیت امور مالی غیرمتمرکز، تیم‌های کوچک پروتکل‌های زیادی را با بودجه محدود ایجاد کرده‌اند و توسعه می‌دهند. این موضوع می‌تواند خطر خطاهای قرارداد را افزایش دهد.

با بررسی پروتکل‌های بزرگ توسط شرکت‌های معتبر حسابرسی، سعی می‌شود نقاط ضعف و خطاها کشف شوند. ماهیت ضد دست‌کاری و تغییرناپذیری بلاکچین می‌تواند باعث شود که پول برای مدت نامحدود در قرارداد هوشمند معیوب قفل شود. اما با ایجاد بسترهای نرم‌افزاری بیشتر برای قراردادهای هوشمند، هرروزه به‌راحتی می‌توانیم ببینیم که شرکت‌های استارت آپ یک لایه انتزاعی ایجاد می‌کنند که قبل از قرارگرفتن در بلاکچین، یک دوره آزمایشی برای قرارداد به شما می‌دهد. این موضوع باید در هنگام سرمایه‌گذاری در قراردادهای هوشمند مورد توجه قرار گیرد. یکی از بزرگترین مزایای امور مالی غیرمتمرکز، یکی از بزرگترین موضوعات آن نیز محسوب می‌شود. به عبارت دیگر، منظور ما، مسئله قابلیت انعطاف‌پذیری آن است. اکنون می‌بینیم این اتفاق چگونه خواهد افتاد.

همان طور که قبلاً ذکر شد، پروتکل‌های امور مالی غیرمتمرکز رایگان و یکپارچه هستند. به این معنی که اکوسیستم امور مالی غیرمتمرکز، وابستگی زیادی به ساختمان بلوک دارد. همچنین برنامه‌ها قابل ترکیب هستند و به‌راحتی با هم کار می‌کنند. پس چرا این موضوع خطر دارد؟ اگر یکی از بلوک‌ها به خوبی کار نکند اکوسیستم تحت‌تأثیر قرار می‌گیرد. این یکی از بزرگترین ریسک‌های کشت‌کنندگان و استخرهای نقدینگی است. شما باید به پروتکلی که

1. whales

پول‌تان را در آن سپرده کرده‌اید و همهٔ اجزایی که در سیستم تعامل دارند، اعتماد کنید.

پلتفرم رمزنگاری کشت سود و پروتکل‌ها

چگونه می‌توانیم بازده کشت سود را به دست آوریم؟ هیچ فرآیند خاصی برای کشت پربازده[1] تعیین نشده است. استراتژی به‌مرور زمان تغییر می‌کند. استراتژی و قوانین در پلتفرم متغیر هستند و هرکدام ریسک‌های ویژه‌ای دارند. هنگام شروع کار به‌عنوان یک کشت‌کنندهٔ تازه‌کار، اولین کاری که باید انجام دهید این است که خود را با عملکرد پروتکل‌های نقدینگی غیرمتمرکز، آشنا کنید.

فرض اصلی این است که وقتی در قراردادهای هوشمند سرمایه‌گذاری می‌کنید در ازای آن پاداش می‌گیرید. اما در واقعیت می‌تواند متفاوت باشد. بنابراین معمولاً پیشنهاد نمی‌شود که به‌عنوان تازه‌کار و بدون اطلاعات اولیه درمورد قوانین و استراتژی‌های کنترل ریسک، بیشتر از پولی سرمایه‌گذاری کنید که توانایی از دست دادن آن را دارید. بنابراین درمورد پلتفرم‌های معروف کشت سود بحث خواهیم کرد. لیست جامعی وجود ندارد، فقط مجموعه‌ای از پروتکل‌ها است که برای توسعه استراتژی کشت سود مهم است.

تأمین مالی کامپاند

کامپاند، مبادلات ارز الگوریتمیک است که مشتریان در آن می‌توانند قرض بگیرند و سرمایه‌گذاری کنند. هرکسی با کیف پول اتریوم می‌تواند در استخر نقدینگی کامپاند سرمایه‌گذاری کند و در ازای مقدار سرمایه‌گذاری، سود دریافت کند. قیمت‌ها بر اساس عرضه و تقاضا طی الگوریتم تعیین می‌شود. کامپاند یکی از مهمترین پروتکل‌ها در تکنولوژی کشت سود است.

کشت سود کامپاند

پلتفرم استفاده شده: میکر[2]، کامپوزیت[3]، کرو[4]، و اینستا داپ[5]

- با بهینه‌سازی برنامه خود با استیبل کوین‌ها، دارایی‌های کامپاند خود را افزایش دهید.

1. high-yielding farming
2. Maker
3. Composite
4. Curve
5. InstaDapp

- والت[1] خود را باز کنید و با وارد کردن اتریوم از طریق اوسیس بارو[2]، (به‌عنوان میکر)، دای دریافت کنید.
- حساب امور مالی غیرمتمرکز هوشمند خود را در اینستا داپ باز کنید و دای را وارد کنید.
- دای‌هایی را که جدید اضافه کردید به بخش کامپوزیت اینستا داپ[3] منتقل کنید.
- از قابلیت «کامپاند حداکثرسازی سود[4]» در اینستا داپ برای بهره گیری از رتبه‌بندی دای برای دارایی دای استفاده کنید.
- آپشن: دای مستقیماً به نقطه اتصال وصل است.
- توجه: وقتی از استراتژی اینستا داپ استفاده می‌کنید، در صورتی که امنیت آن زیر حد آستانه باشد ممکن است شکست بخورد. نسبتی که در این استراتژی توصیه می‌شود ٪۶۰ است.

میکردائو

میکر، پلتفرم وام‌دهی غیرمتمرکز است که از ایجاد دای حمایت می‌کند و استیبل کوینی است که به‌صورت الگوریتمی به ارزش دلار آمریکا وابسته است. کاربران می‌توانند میکر والتی[5] باز کنند تا دارایی‌هایی مثل اتریوم، بت[6]، یو.اس.دی.سی و دبلیو.بی.تی.سی را قفل کنند. آن‌ها می‌توانند دای را به‌عنوان وام در مقابل بهادار وثیقه‌شده ایجاد کنند. این مبلغ اضافه، به منزلهٔ بهره‌ای است که به نام شارژ ثابت[7] شناخته می‌شود که توسط دارندگان توکن میکر تعیین می‌شود. کشت کنندگان سود می‌توانند از دای مینت میکر[8] برای استراتژی کشت سود خود استفاده کند.

سینتتیکس[9]

سینتتیکس در واقع پروتکل دارایی مصنوعی است. هرکسی می‌تواند به‌صورت ایمن سپرده‌گذاری کند و با توکن شبکه سینتتیکس یا اتریوم سپرده کند و دارایی سینتتیکس برای آن منتشر کند. اما دارایی مصنوعی چیست؟ تقریباً هرچیزی یک جریان استیبل قیمتی دارد

1. Vault
2. Oasis Borrow
3. InstaDapp Composite
4. Maximize Profit COMP
5. Vault Maker
6. BAT
7. stability charge
8. DAI Mint Maker
9. Synthetix

که به شما اجازه می‌دهد به‌صورت مجازی دارایی مالی را به پلتفرم سینتتیکس اضافه کنید. سینتتیکس می‌تواند برای همه نوع دارایی استفاده شود که برای کشت سود ایجاد می‌شوند. اگر قصد دارید از محتوی طلا[1] برای بلندمدت جهت کشت سود استفاده کنید، دارایی مصنوعی آپشن‌های مناسبی دارد.

آوه

پروتکل وام‌دهی غیرمتمرکز و سپرده‌گذاری است. نرخ بهره به‌صورت الگوریتمی بر اساس شرایط بازار تعیین می‌شود. وام‌دهندگان در ازای مبلغی که می‌دهند توکن دریافت می‌کنند. این رمزنگاری سپرده شده، سود تولید می‌کند و به سود مرکب سپرده اضافه می‌شود. همچنین آوه می‌تواند از ویژگی‌های دیگری مانند نرخ بهره استفاده کند. آوه که پروتکل وام‌دهی و وام‌دهی غیرمتمرکز به‌صورت گسترده است، توسط گسترش‌دهندگان محصولات[2] مورد استفاده قرار می‌گیرد.

یونی سواپ

یونی سواپ، پروتکل دیکس یا صرافی غیرمتمرکز[3] است که اجازه می‌دهد توکن‌های غیرقابل‌اعتماد را در آن معامله کنید. ارائه‌دهندگان نقدینگی برای ایجاد پلتفرم معامله ارزش برابر، دو توکن مختلف را در نظر می‌گیرند. سپس معامله‌گران می‌توانند در این استخر نقدینگی معامله کنند. برای تأمین نقدینگی معاملات، ارائه‌دهندگان نقدینگی برای مبادلاتی که انجام می‌شود کارمزد دریافت می‌کنند. به دلیل ماهیت بی‌دردسر[4] یونی سواپ به‌صورت گسترده برای مبادله توکن‌های نامطمئن استفاده می‌شود. استفاده از یونی سواپ یا متدهای مشابه استراتژی مفیدی برای کشت سود است.

پلتفرم کرو فایننس[5]

کرو فایننس، پروتکل مبادله غیرمتمرکز است که به‌صورت منحصربه‌فرد برای مبادله ارزهای ثابت طراحی شده است. برخلاف سایر پروتکل‌های مشابه یونی سواپ، کرو به کاربران اجازه

1. gold bag
2. crop growers
3. decentralized exchange
4. hassle-free
5. Curve Finance

می‌دهد کوین‌های ثابت گران‌قیمت را با افت نسبتاً کمتری مبادله کنند. همان طور که حدس می‌زنید، استخر کرو به دلیل غنی بودن از استیبل کوین‌ها قسمت مهمی از چهارچوب کشت سود است.

کرو، پلتفرم میکر بازار اتوماتیک محبوبی است که روش‌های مفیدی برای بازخرید توکن‌ها با کارمزد کم ارائه می‌دهد. به‌واسطهٔ حمایت استخر نقدینگی بر پایه دارایی، شامل کمترین افت است. درحالی‌که این روش هزینهٔ ارائه‌دهندگان نقدینگی را که استخرهای توکن را ارائه می‌دهند کاهش می‌دهد، کرو با ادغام با پروتکل‌های خارجی امور مالی غیرمتمرکز و ایجاد سود در فرم سی.آر.وی و نرخ بهره توکن، کاربران را تشویق می‌کند.

کشت سود با استفاده از بیت‌کوین کرو[1]

پلتفرم از پروتکل رن[2]، کرو، سینستیکس و بالانسر استفاده می‌کند، تا ضمن به دست آوردن سی.آر.وی، بال، رن، اس.ان.ایکس، نقدینگی بیت‌کوین استخر کرو را نیز تضمین کند.

- انتقال بیت‌کوین به اتریوم با استفاده از پل رن[3]
- بیت‌کوین رن جدید را وارد «اس.بیت کوین» در استخر کرو کنید.
- بلیط‌های اس.بیت کوین را در مینتر[4] برای بخش سود تأمین‌کنندگان نقدینگی ثبت کنید.
- قیمت‌ها را در فرم توکن‌های بالانس‌کننده[5] اس.ان. ایکس/رن به دست آورید.
- سودهای اس.ان.ایکس و یا رن را از روی ترازنامه خود به دست آورید.

استخراج نقدینگی پلتفرم کرو با استفاده از خود کرو ، سینتتیکس، پروتکل رن و وای.یارن[6] انجام می‌شود. درآمد ناشی از سی.آر.وی را با شاخص نقدینگی «کرو دائو» و «کرو» افزایش دهید.

- وثیقه خود را به یکی از استخرهای نقدینگی کرو پرداخت کنید.
- کسانی که می‌خواهند در استخر بیت‌کوین شرکت کنند با استفاده از پروتکل رن بیت‌کوین را به اتریوم انتقال دهند.
- در توکن‌های نقدینگی در کرو سرمایه‌گذاری کنید.

---

1. Bitcoin Curve
2. Ren
3. Ren Bridge
4. Mintr
5. balancing tokens
6. yEarn

- برای افزایش نقدشوندگی، سی.آر.وی را امن و با استفاده از کرو دائو آنرا قفل می‌کنیم.
- انگیزه‌های اضافه‌ای مانند اس.ان.ایکس و رن برای استخرهای یو.اس.دی و اس.بیت‌کوین پیدا کنید.

کرو در واقع، یک پلتفرم بازارساز[1] اتوماتیک شبیه یونی سواپ و بالانسر است با این تفاوت که از استخرهای نقدینگی شامل دارایی‌هایی با رفتار مشابه مثل کوین‌های ثابت و یا یو پکیج‌های[2] مشابه مانند دبلیو.بیت کوین و تی.بیت کوین، استفاده می‌کند. این رویکرد به کرو اجازه می‌دهد الگوریتم‌های مفیدی استفاده کند و کارمزد و افت و نوسان کمی در هرگونه معاملات غیرمتمرکز اتریوم دارد.

بالانسر

بالانسر، پروتکل نقدینگی کرو و یونی سواپ است. البته مهم‌ترین تفاوت آن این است که وجوه نقدینگی می‌توانند توزیع توکن‌ها را تنظیم کنند. این موضوع به تأمین‌کنندگان نقدینگی اجازه می‌دهد به‌جای سهم مساوی ۵۰/۵۰ مورد نیاز توسط یونی سواپ، استخر بالانس مورد نظر خود را ایجاد کنند. تأمین‌کنندگان نقدینگی نیز مانند یونی سواپ، برای مبادلاتی که در وجوه نقدینگی انجام می‌گردد، کارمزد دریافت می‌کنند.

بالانسر با قابلیت انعطاف در ایجاد نقدینگی، یکی از مهم‌ترین نوآوران در زمینهٔ استراتژی‌های رشد محصولات[3] است.

استخراج نقدینگی توسط بالانسر

پلتفرم موردنظر، سرمایه شما را به استخر نقدینگی بالانسر برای تولید توکن‌های کنترلی[4] بال[5] متصل می‌کند. برای تعیین اینکه کدام استخر بیشترین بال‌ها را بر اساس درصد کل دریافت می‌کند، از یک جدول پیش‌بینی مانند پیش بینی مبادلات استفاده کنید، جایی که ۱ بالاترین نسبت ممکن را دارد.

- سایت https://pools.balancer.exchange/#/ را مشاهده کنید و در استخر مورد نظر

1. market maker
2. u-packaging
3. crop growing strategies
4. control tokens
5. BAL

سرمایه گذاری کنید.

- توصیه: استخری که موقتا ضرر را کاهش میدهد، توصیه می‌شود که شامل استخرهای با اتصال ۱:۱ است؛ مانند:«اس. اتریوم/دبلیو اتریوم»، «اس.بیت کوین/ دبلیو.بیت کوین» و «دای/یو.اس.دی.سی».

یرن فایننس[1]

یرن فایننس، اکوسیستم غیرمتمرکز برای خدمات اعتباری نظیر آوه ، کامپاند و... است. هدف آن یافتن سودآورترین خدمات وام به طور الگوریتمی و بهینه‌سازی وام‌دهی رمزگذاری[2] است. در سپرده‌گذاری، پول نقد به توکن‌ها تبدیل می‌شوند و به‌طور منظم بالانس می‌شوند تا سود را به حداکثر برسانند. یرن فایننس، برای کشت‌کنندگانی مفید است که به دنبال پروتکلی هستند که به‌صورت اتومات بهینه‌ترین استراتژی را انتخاب می‌کند.

1. Yearn Finance
2. crypto loaning

فصل ۶

راه‌های استخراج بیت‌کوین شما, توسط خود شما

*سه روش برای به دست آوردن بیت‌کوین وجود دارد؛ با خرید در بورس، یا از طریق جمع‌آوری آن‌ها برای کالاها و خدمات و آخرین مورد از طریق استخراج کالاهای جدید است. بیت‌کوین مانند پول نقد عمل می‌کند اما می‌تواند به طلا استخراج شود. استخراج در واقع ادبیات مورد استفاده برای کشف بیت‌کوین‌های جدید است؛ درست مثل اکتشاف طلا. معاملات بیت‌کوین در یک بلوک با اندازه ثابت جمع شده و به مانند زنجیره بلوک در زندگی واقعی به آن‌ها اضافه می‌شود. برای مثال، سینتیا[1] از یک خرده‌فروش آنلاین با بیت‌کوین یک تلویزیون خریداری می‌کند. ماینرها برای اطمینان از واقعی بودن بیت‌کوین وی، یک عمل محاسباتی انجام می‌دهند که مختص هر بلاکچین است تا معاملات را تأیید و بلوک‌های جدید معاملات را اضافه کند.

*معاملات روند اعتبار سنجی پیچیده تر از آن است، اما برای ساده‌سازی آن، ما با ساده‌ترین کلمات به‌عنوان اعتبار معاملات فکر می‌کنیم. تمام معاملات در بلوک‌هایی با یک قفل مجازی به نام بلاکچین تنظیم می‌شوند. ماینرها سپس نرم‌افزار مناسب را برای یافتن کلید اجرا می‌کنند. این کلید به جهت بازکردن قفل مذکور مناسب بوده و در ادامه، بلوک‌های جدیدی اضافه می‌شود. وقتی رایانهٔ آن‌ها، این کلید را پیدا می‌کند، جعبه باز می‌شود و معاملات تأیید خواهد شد. پاداش در نظر گرفته شده برای یافتن کلید مناسب، برای باز کردن قفل به میزان ۱۲,۵ بیت‌کوینِ تازه تولید شده است. آن مقدار نیمی از تعداد مشخصی از بلوک‌ها است. دلیل این امر، قوانین از پیش تعیین‌شده

1. Cynthia

برای بیت‌کوین است که توسط مخترعی به نام ساتوشی ناکاموتو[1] ایجاد شده است. با توجه به نظر یک سایت معتبر برای آخرین معاملات واقعی بیت‌کوین، تعداد آزمایشی که در حال حاضر برای پیدا کردن کلید انجام می‌شود، در حدود ۱،۷۸۹،۵۴۶،۹۵۱،۰۵ است. صرف‌نظر از تعداد زیاد آزمایشات، پاداش ۲۵ بیت‌کوین تقریباً هر ده دقیقه ارائه می‌شود. بااین‌حال، استخراج انفرادی باعث تضعیف روحیه می‌شود. زیرا فرآیند جست‌وجوی بلوک‌ها بسیار مشهور و رایج است، و مشکل یافتن یک بلوک کمتر از آن است که شما بخواهید آن را برای مدت مثلاً سه سال پیش از تولید هر سکه‌ای، کنار بگذارید. از طرف دیگر، استخراج تلفیقی[2] بسیار مفیدتر است. به شما این امکان را می‌دهد که کار را در میان مردم تقسیم کنید. تمام کاری که شما نیاز دارید این است که برای سهام در یک بلوک کار کنید. (سهم‌هایی که در یک بلوک به اشتراک گذاشته می‌شود)، وقتی که استخراج شده و به زنجیره بلوک یا همان بلاکچین ضمیمه می‌شود، شما بر اساس تعداد افراد یا کاربرانی که دارید درصدی از بلوک را دریافت می‌کنید. در اینجا هزینه‌های کمتری نیز شامل می‌شود. در ادامه چند گام وجود دارد که باید انجام دهید تا بتوانید با آن استخراج بیت‌کوین خود را به‌راحتی شروع کنید.

کیف پول بگیرید

شما می‌توانید کیف پول خود را به‌صورت محلی یا آنلاین ذخیره کنید. شما نیاز دارید برای استفاده یا دانلود یک پرونده بلاکچینِ نسبتاً بزرگ، در حدود ۳۲۰ گیگابایت داشته باشید. دانلود و به‌روزرسانی کیف پول محلی ممکن است منفی و غیرممکن باشد. روشی که شما تصمیم می‌گیرید برای نگه داشتن بیت‌کوین خود استفاده کنید، کاملاً به شخص شما بستگی دارد. هرچند، هیچ نوع کیف پول کاملی وجود ندارد؛ زیرا همهٔ آن‌ها جنبه‌های مثبت و منفی دارند؛ بااین‌حال، طرفداران حفظ حریم خصوصی کیف پول محلی را ترجیح می‌دهند. لحظه‌ای که هرکدام از کیف پول‌ها را که دوست دارید ایجاد کنید، یک آدرس مانند زیر دریافت می‌کنید:

1BEkUGADFbrEShQb9XJ

این روش مستقیم برای ارسال بیت‌کوین به کیف پول‌تان است، پس آن را یادداشت کنید.

1. Satoshi Nakomoto
2. Pooled Mining

شما می‌توانید آدرس کیف پول تحت حساب‌های مرتبط در کوین بیس [1]را پیدا کنید.

به استخر بپیوندید

قبل از اینکه بتوانید در استخر استخراج کنید، باید با سایر استخراج‌کنندگان در بلوک‌های موجود کار کنید. هر استخر بیشتر با هزینه‌هایی که توسط بلوک دریافت شده و همچنین با تعداد کاربران، متمایز می‌گردد. استخرهایی که تعداد کاربران کمتری دارند نیز می‌توانند زمان کمتری داشته باشند برای کشف بلوک‌هایی که باید استخراج شوند. اما استخرهای با تعداد زیاد کاربر، معمولاً به پرداخت‌های کمتری ختم می‌شوند. دستورالعمل‌های ساده‌ای برای اغلب سرویس‌ها وجود دارد تا از غرق شدن جلوگیری شود. همچنین مطمئن شوید که آدرس کیف پول خود را در اطلاعات استخر وارد کرده‌اید. این باعث اطمینان می‌شود که بیت‌کوین خود را به دست آورده‌اید.

استخراج کن

گزینه‌های مختلف استخراج برای انجمن‌های مختلف وجود دارد، و کاربران او.اس.ایکس[2] ممکن است خودشان را در دردسر ببینند. ماینرها از چرخه‌های جی.پی.یو[3] اضافی استفاده کرده تا عملیات استخراج را تأمین کنند. ماینرها از این چرخه برای مراقبت از فرآیندهای کاربر به کاربر مربوط به بیت‌کوین استفاده می‌کنند. بنابراین، شما در حال کار با شبکه و همچنین انجام «کار» می‌توانید بیشتر در مورد این موضوع تحقیق کنید تا یک تصویر واضح‌تر به دست آورید. برای اینکه نقطهٔ شروع را به شما نشان دهیم، واژهٔ آسیک[4] را جست‌وجو کنید (مدارهای یکپارچه خاص اپلیکیشن[5]).

تمرکز حواس شما به جایزه باشد (پول شما)

استفاده و استخراج بیت‌کوین بسیار ساده است. ممکن است فکر کنید که قادر به عبور از ماشین‌های زیادی با هم باشید و بیت‌کوین را مثل شن و ماسه جمع کنید، اما این‌طور نیست.

1. Coinbase
2. OSX
3. GPU
4. Asic
5. Application Specific Integrated Circuits

هرچه بیت‌کوین بیشتری کشف شود، پیدا کردن آن‌ها دشوارتر می‌شود. با استفاده از یکی از ماشین‌حساب‌های سودآور آنلاین برای استخراج بیت‌کوین یا اتریوم، می‌فهمید در برابر چه چیزی مخالفت می‌کنید. به‌طور خلاصه، اگر هزینهٔ اجرای سخت‌افزار شما بیش از سود شما در بیت‌کوین است، آن وقت شما به احتمال زیاد کار اشتباهی انجام داده‌اید.

نتیجه‌گیری

حلقه های نظام مالی غیرمتمرکز در اطراف برنامه‌های کاربردی که به داپس[1] معروف است، قرار دارد. به عبارت دیگر، آن‌ها را اپلیکیشن‌های غیرمتمرکز می‌نامیم. این اپلیکیشن‌ها برای انجام وظایف و کارکردهای مالی در دفاتر کل حسابداری دیجیتال پیشگام هستند که با عنوان بلاکچین نیز شهرت دارند. بلاکچین یک تکنولوژی است که برای اولین بار توسط بیت‌کوین به کار گرفته شد، اما از آن زمان به بعد وسیع‌تر شده است. به‌جای معاملات انجام‌شده که توسط یک واسطهٔ متمرکز مانند صرافی رمزارز نگاری (ارز دیجیتال) انجام می‌شود، معاملات به‌طور مستقیم بین افراد انجام می‌شود. بااین‌حال، با کمک برنامه‌های قراردادهای هوشمند است. داپس از طریق افزونه‌های مرورگر وب‌کم تری[2] یا برنامه‌هایی مانند متاماسک قابل دسترسی هستند که به کاربران اجازه می‌دهد تا با بلاکچین اتریوم از طریق وب‌سایت ارتباط برقرار کنند. علاوه بر این، اغلب این داپس‌ها می‌توانند به یکدیگر برای ایجاد خدمات مالی دقیق متصل شده و کار کنند. برای مثال، یک نگهدارنده سکه ثابت می‌تواند دارایی را به یک استخر نقدینگی تبدیل کند. سایرین با قرار دادن وثیقهٔ بیشتر، معمولاً بیش از مقدار وام، از این استخر وام می‌گیرند. سپس این سیاست، نرخ بهره را بر اساس ادعای زمان تا زمان برای دارایی تغییر می‌دهد.

تمرکززدایی به معنای عدم وجود صرافی مرکزی است. برنامه‌های قراردادهای هوشمند که برای سیاست‌های نظام مالی غیرمتمرکز مورد استفاده قرار می‌گیرند با کمک نرم‌افزار منبع باز، برای جامعه توسعه‌دهندگان و برنامه‌نویسان عملیاتی می‌شوند. یک نمونه از سیاست نظام مالی غیرمتمرکز، یونی سواپ است. این یک صرافی غیرمتمرکز یا دیکس است که روی بلاکچین اتریوم کار می‌کند و اجازهٔ تجارت صدها توکن دیجیتال مختلف را می‌دهد که در زنجیرهٔ بلوک اتریوم تولید می‌شود.

1. DApps
2. WebCam3

به‌جای اینکه به نشانگرهای بازار متمرکز برای پُرکردن سفارشات وابسته شوید، الگوریتم یونی سواپ، کاربران را به ایجاد استخرهای نقدینگی برای رمز ارزها ترغیب می‌کند. این کار از طریق تولید هزینه‌های تجاری است برای افرادی که نقدینگی را تأمین می‌کنند. درحالی‌که کاربران کاملاً سیستم‌عامل یونی سواپ را کنترل می‌کنند، یک تیم توسعه مسئول نوشتن نرم‌افزار برای استقرار آن است.

خرید مستقیم تنها نوع معامله یا قراردادی نیست که توسط آن‌ها کنترل می‌شود. شرکت‌های بزرگ، برنامه‌های مالی دیگر مانند وام، بیمه، مشتقات، شرط‌بندی، سرمایه‌گذاری جمعی و چند مورد دیگر را نیز در اختیار خود دارند.

بنابراین، دورکردن واسطه‌ها از تمام این نوع معاملات یکی از اهداف اصلی نظام مالی غیرمتمرکز است. ما آخرین ارزهای رمزنگاری‌شده، مانند کشاورزی رمزنگاری‌شده و محصولات نظام مالی غیرمتمرکز را پوشش دادیم. چه چیز دیگری می‌تواند این انقلاب اقتصادی پیشرفته را به ارمغان بیاورد؟ ما می‌دانیم که برنامه‌های جدید بر اساس این اجزای فعلی چه کاربردهای جدیدی خواهند داشت. بااین‌حال، پروتکل‌های نقدینگی غیرقابل اطمینان و سایر محصولات نظام مالی غیرمتمرکز در خط مقدم اقتصاد، علم اقتصاد رمزنگاری و علم رایانه قرار دارند. بی‌شک بازار پول نظام مالی غیرمتمرکز، می‌تواند به ایجاد یک سیستم مالی باز و قابل دسترسی کمک کند که هرکسی با یک ارتباط اینترنتی بتواند به آن دسترسی داشته باشد. در نتیجه شکاف بین زندگی ما روی زمین را پر می‌کند و بر عامل انسانی برای رسیدن به زندگی در مریخ اتکا دارد. درعین‌حال، ما درآمد انفعالی حاصل از کشت سود را روی اوراق بهادار مبتنی بر زمین تولید می‌کنیم. در بخش‌های آینده مجموعه کتاب « Stake Hodler »، ما قصد داریم بسیاری از برنامه‌های کاربردی زنجیرهٔ بلوک در عمق را پوشش دهیم. از جمله می‌توان به قراردادهای هوشمند، اینترنت اشیا، خرده‌فروشان، کشاورزی و تولید اشاره کرد.